# 中金金融认证中心全球信任体系
# 证书策略和电子认证业务规则

**（CFCA Global-Trust CP/CPS）**

V4.10



2025 年 11 月 3 日

# 版本控制表

| 版本 | 修改状态 | 修改说明 | 修改人 | 审核人/批准人 | 生效期 |
|---|---|---|---|---|---|
| 1.0 | 形成版本并审核通过 | | | CFCA 安委会 | 2011 年 06 月 |
| 2.0 | 添加 | 增加了 EV 系统、OCA21 的相关描述及要求，增加了证书类型描述及证书密钥等描述，将版本升级为 2.0，形成初稿 | 赵改侠 | | |
| | 修改 | 根据 2013 年 4 月 7 日安委会评审结论修改相关内容 | 赵改侠 | CFCA 安委会 | 2013 年 4 月 |
| 2.1 | 修改 | 依据 BR 的补充相关条款 | 赵改侠 | CFCA 安委会 | 2014 年 3 月 |
| 3.0 | 修订 | 发布了 GT 系统 sha1 密码算法的策略，增加了 EV Codesign OCA 系统、OV OCA、OV CodeSign OCA 系统证书策略 | 张翼、赵改侠 | CFCA 安委会 | 2015 年 8 月 |
| 3.1 | 修订 | 更改 EV CodeSign、OV SSL、OV CodeSign 证书策略 OID | 张翼 | CFCA 安委会 | 2015 年 8 月 |
| 3.2 | 修订 | 根据 2016 年 6 月 24 日安委会评审结论修改相关内容 | 赵烨昕 | CFCA 安委会 | 2016 年 6 月 |
| 3.3 | 修订 | 删除 CFCA GT CA 及 OCA2、OCA21 等系统及所发放证书的相关内容，CFCA GT OCA2 在 2016 年 1 月 1 日后不再签发证书，CFCA OCA2 的业务将由 CFCA OV OCA 承接。CFCA OCA21 在 CFCA 电子认证业务规则中描述；增加 CAA 查询的声明。更正了版本信息 | 孙圣男 | CFCA 安委会 | 2017 年 9 月 |
| 4.0 | 修订 | 删除了关于 EV 代码签名证书、OV 代码签名证书的说明；增加关于证书中嵌入证书透明度信息的说明；调整文档结构并根据 CA/B 论坛要求调整验证资料及验证方法的说明 | 孙圣男 | CFCA 安委会 | 2019 年 6 月 |
| 4.1 | 修订 | 根据部门职能调整，修改职能分工；删除 CFCA EV SM2 OCA 及 CFCA OV SM2 OCA 等系统及所发放证书相关内容；增加 CFCA Global ECC ROOT CA1、CFCA Global RSA ROOT CA1 及 CFCA EV ECC OCA1、CFCA OV ECC OCA1、CFCA EV OCA1、CFCA OV OCA1 相关内容；自 2020 年 9 月 1 日起，不再发放有效期超过 398 天服务器证书；修订错误性文字描述 | 毕鑫龙 | CFCA 安委会 | 2020 年 7 月 |

| | | | | | |
|---|---|---|---|---|---|
| 4.2 | 修订 | 更新 Mozilla 证书策略，根据 RFC3647 更新目录章节及内容；增加 DV SSL 证书内容；修订错误性文字描述 | 毕鑫龙 | CFCA 安委会 | 2021 年 7 月 |
| 4.3 | 修订 | 根据 BR，更新身份识别与鉴定，修订名称唯一性说明，补充数据源准确性和 CAA；调整证书吊销内容；添加证书不再包含 OU 的说明 | 仇大伟 | CFCA 安委会 | 2022 年 7 月 |
| 4.4 | 修订 | 更新本文档为“中金金融认证中心全球信任体系证书策略和电子认证业务规则”；调整 CP/CPS 更新频率；调整 CAA 章节位置 | 仇大伟 | CFCA 安委会 | 2022 年 11 月 |
| 4.5 | 修订 | 修改策略管理联系方式；修订部分内容描述 | 王若涵 | CFCA 安委会 | 2023 年 9 月 |
| 4.6 | 修订 | 将附录中定义和缩略词调整至 1.6 章节；修订机构身份鉴别；修订域名鉴别；修订证书批准和拒绝；修订证书签发增加 linting；修订证书配置要求；修订审计与评估 | 仇大伟<br>李开瑞<br>高佩艳<br>赵莎 | CFCA 安委会 | 2024 年 8 月 30 日 |
| 4.7 | 修订 | 在 1.5.2 章节增加 CPR 表单描述并修改 11.3 章节部分文字错误 | 宋鑫磊<br>许盛晨<br>高佩艳 | CFCA 安委会 | 2025 年 5 月 30 日 |
| 4.8 | 修订 | 调整域名控制权验证方法并审核修订其他内容 | 宋鑫磊<br>许盛晨<br>高佩艳<br>郑晓娟 | CFCA 安委会 | 2025 年 7 月 21 日 |
| 4.9 | 修订 | 自审修订 | 宋鑫磊<br>许盛晨<br>高佩艳<br>郑晓娟 | CFCA 安委会 | 2025 年 10 月 25 日 |
| 4.10 | 修订 | 调整根及中间根名称 | 宋鑫磊<br>高佩艳 | CFCA 安委会 | 2025 年 11 月 3 日 |

# 目　　录

# 1 概括性描述

## 1.1 概述

中金金融认证中心有限公司（China Financial Certification Authority，英文简称 CFCA），于 2000 年 6 月 29 日正式挂牌成立，是经中国人民银行牵头组建、国家信息安全管理机构批准成立的国家级权威的安全认证机构，是重要的国家金融信息安全基础设施之一，也是《中华人民共和国电子签名法》颁布后，国内首批获得电子认证服务许可资质的电子认证服务机构之一。

证书策略（CP, Certificate Policy）是认证机构（CA, Certification Authority）制订的一组策略，表明 CFCA PKI 体系中的各个参与者的划分与其义务，并包含 CFCA 证书基本策略。

电子认证业务规则（CPS, Certification Practice Statement）是关于认证机构（CA, Certification Authority）在全部数字证书（以下简称证书）服务生命周期（如签发、吊销、更新）中的业务实践所遵循规范的详细描述和声明，是对相关业务、技术和法律责任方面细节的描述。

本 CP/CPS 是 CFCA 全球信任体系下的证书策略和电子认证业务规则。

本文档的编写遵从《中华人民共和国电子签名法》、GB/T 25056《证书认证系统密码及相关安全技术规范》、《电子认证服务密码管理办法》、中华人民共和国工业和信息化部颁布的《电子认证服务管理办法》、《电子认证业务规则规范(试行)》，以及最新的 RFC 3647、《Webtrust 安全审计规范》、《EV 证书指导准则》、《Baseline-Requirements》及 CA 的一般运作规范。

CFCA 遵循 WebTrust 相关要求，并通过外部审计师审计； CFCA 获取了

主管单位中华人民共和国工业和信息化部颁发的电子认证服务许可等资质，并处于资质有效期内。

若本文件与适用行业指南或标准（以下简称 “适用要求”）的规范性条款存在任何不一致之处，则适用要求优先于本 CP/CPS。



## 1.2 文档名称与相关标识

此文档的名称为《CFCA 全球信任体系证书策略和电子认证业务规则(CFCA Global-Trust CP/CPS)》。

### 1.2.1 证书策略标识

CFCA 向国家 OID 注册管理中心注册了相应的对象标识符（OID），本文档涉及到的证书 OID 如下：

| 序号 | 对象标识符种类 | 对象标识符 | 描述 |
|---|---|---|---|
| 1 | 文档标识 | 2.16.156.112554.2 | CFCA 全球信任体系证书策略和电子认证业务规则 |
| 2 | 证书标识 | 2.16.156.112554.3 | EV SSL 服务器证书 |
| 3 | 证书标识 | 2.23.140.1.1 | EV SSL 服务器证书（Baseline Requirement 要求） |

| | | | |
|---|---|---|---|
| 4 | 证书标识 | 2.16.156.112554.4.1 | OV SSL 服务器证书 |
| 5 | 证书标识 | 2.23.140.1.2.2 | OV SSL 服务器证书<br>（Baseline Requirement 要求） |
| 6 | 证书标识 | 2.16.156.112554.4.3 | DV SSL 服务器证书 |
| 7 | 证书标识 | 2.23.140.1.2.1 | DV SSL 服务器证书<br>（Baseline Requirement 要求） |
| 8 | 扩展域标识 | 1.3.6.1.4.1.11129.2.4.2 | 证书透明度日志<br>（各主流根证书库要求） |

## 1.2.2修订

| 版本 | 修改状态 | 修改说明 | 生效期 |
|---|---|---|---|
| 1.0 | 形成版本并审核通过 | | 2011 年 06 月 |
| 2.0 | 添加 | 增加了 EV 系统、OCA21 的相关描述及要求，增加了证书类型描述及证书密钥等描述，将版本升级为 2.0，形成初稿 | |
| | 修改 | 根据 2013 年 4 月 7 日安委会评审结论修改相关内容 | 2013 年 4 月 |
| 2.1 | 修改 | 依据 BR 的补充相关条款 | 2014 年 3 月 |
| 3.0 | 修订 | 发布了 GT 系统 sha1 密码算法的策略，增加了 EV Codesign OCA 系统、OV OCA、OV CodeSign OCA 系统证书策略 | 2015 年 8 月 |
| 3.1 | 修订 | 更改 EV CodeSign、OV SSL、OV CodeSign 证书策略 OID | 2015 年 8 月 |
| 3.2 | 修订 | 根据 2016 年 6 月 24 日安委会评审结论修改相关内容 | 2016 年 6 月 |
| 3.3 | 修订 | 删除 CFCA GT CA 及 OCA2、OCA21 等系统及所发放证书的相关内容，CFCA GT OCA2 在 2016 年 1 月 1 日后不再签发证书，CFCA OCA2 的业务将由 CFCA OV OCA 承接。CFCA OCA21 在 CFCA 电子认证业务规则中描述；增加 CAA 查询的声明。更正了版本信息 | 2017 年 9 月 |
| 4.0 | 修订 | 删除了关于 EV 代码签名证书、OV 代码签名证书的说明；增加关于证书中嵌入证书透明度信息的说明；调整文档结构并根据 CA/B 论坛要求调整验证资料及验证方法的说明 | 2019 年 6 月 |
| 4.1 | 修订 | 根据部门职能调整，修改职能分工；删除 CFCA EV SM2 OCA 及 CFCA OV SM2 OCA 等系统及所发放证书相关内容；增加 CFCA Global ECC ROOT CA1、CFCA Global RSA ROOT CA1 及 CFCA EV ECC OCA1 、CFCA OV ECC OCA1、CFCA EV OCA1、CFCA OV OCA1 相关内容；自 | 2020 年 7 月 |

| | | | |
|---|---|---|---|
| | | 2020 年 9 月 1 日起，不再发放有效期超过 398 天服务器证书；修订错误性文字描述 | |
| 4.2 | 修订 | 更新 Mozilla 证书策略，根据 RFC3647 更新目录章节及内容；增加 DV SSL 证书内容；修订错误性文字描述 | 2021 年 7 月 |
| 4.3 | 修订 | 根据 BR，更新身份识别与鉴定，修订名称唯一性说明，补充数据源准确性和 CAA；调整证书吊销内容；添加证书不再包含 OU 的说明 | 2022 年 7 月 |
| 4.4 | 修订 | 更新本文档为“中金金融认证中心全球信任体系证书策略和电子认证业务规则”；调整 CP/CPS 更新频率；调整 CAA 章节位置 | 2022 年 11 月 |
| 4.5 | 修订 | 修改策略管理联系方式；修订部分内容描述 | 2023 年 9 月 |
| 4.6 | 修订 | 将附录中定义和缩略词，调整至 1.6 章节；修订机构身份鉴别；修订域名鉴别；修订证书批准和拒绝；修订证书签发增加 linting；修订证书配置要求；修订审计与评估 | 2024 年 8 月 30 日 |
| 4.7 | 修订 | 在 1.5.2 章节增加 CPR 表单描述并修改 11.3 章节部分文字错误 | 2025 年 5 月 30 日 |
| 4.8 | 修订 | 调整域名控制权验证方法并审核修订其他内容 | 2025 年 7 月 21 日 |
| 4.9 | 修订 | 自审修订 | 2025 年 10 月 25 日 |
| 4.10 | 修订 | 调整根及中间根名称 | 2025 年 11 月 3 日 |

## 1.3 PKI 参与者

本文中所包含的电子认证活动参与者有：电子认证服务机构、注册机构、订户、依赖方以及其它参与者，下面将分别进行描述。

### 1.3.1 电子认证服务机构

电子认证服务机构 CA（Certification Authority）承担证书签发、更新、吊销、密钥管理、证书查询、证书黑名单（又称证书吊销列表或 CRL）发布、政策制定等工作，本文中仅指 CFCA。

### 1.3.2 注册机构

注册机构 RA(Registration Authority)负责订户证书的申请受理、审批和管理，

直接面向证书订户，并负责在订户和 CA 之间传递证书管理信息。

CFCA 全球信任体系下的 CFCA EV OCA、CFCA OV OCA、CFCA DV OCA、CFCA EV ECC OCA G2、CFCA OV ECC OCA G2、CFCA DV ECC OCA G2、CFCA EV RSA OCA G2、CFCA OV RSA OCA G2、CFCA DV RSA OCA G2 的注册机构设在 CFCA 内部，由 CFCA 本身承担 RA 职责，不委托其它机构行使此职责。

### 1.3.3 订户

订户是指向 CFCA 申请数字证书的实体。

需要明确的是，证书订户与证书主体是两个不同的概念。“证书订户”是指向 CFCA 申请证书的实体，通常为个人或机构；“证书主体”是指与证书信息绑定的实体，服务器证书中的“证书主体”通常是指受信任的服务器或用于确保与某一机构安全通信的其它设施。证书订户需要承担相应的责任与义务，而证书主体则是证书所要证明的可信赖方。

### 1.3.4 依赖方

依赖方是指信赖于证书所证明的基础信任关系并依此进行业务活动的实体。

### 1.3.5 其它参与者

以上未提及的，在整个 CFCA 和其服务架构内参与证书服务提供的其它实体。

## 1.4 证书应用

### 1.4.1 CFCA 全球信任证书类型及适合的证书应用

| 签发 CA | 证书类型 |
|---|---|
| CFCA EV OCA | EV SSL 全球服务器证书(RSA 算法) |
| CFCA OV OCA | OV SSL 全球服务器证书(RSA 算法) |
| CFCA DV OCA | DV SSL 全球服务器证书(RSA 算法) |
| CFCA EV ECC OCA G2 | EV SSL 全球服务器证书(ECC 算法) |
| CFCA OV ECC OCA G2 | OV SSL 全球服务器证书(ECC 算法) |
| CFCA DV ECC OCA G2 | DV SSL 全球服务器证书（ECC 算法） |
| CFCA EV RSA OCA G2 | EV SSL 全球服务器证书(RSA 算法) |
| CFCA OV RSA OCA G2 | OV SSL 全球服务器证书(RSA 算法) |
| CFCA DV RSA OCA G2 | DV SSL 全球服务器证书(RSA 算法) |

CFCA EV ROOT、CFCA Global ECC ROOT G2、CFCA Global RSA ROOT G2 仅用于签发下级 CA 证书，不签发最终订户证书。

#### 1.4.1.1 CFCA EV SSL 全球服务器证书

CFCA EV SSL 全球服务器证书包含单域名证书、多域名证书，该类证书适合用于在订户浏览器与 Web 服务器之间建立安全通道，实现数据信息在客户端与服务器之间的加密传输，防止数据信息的泄露。

CFCA EV SSL 全球服务器证书由 CFCA EV OCA、CFCA EV RSA OCA G2、CFCA EV ECC OCA G2 签发 SHA256 证书，密钥长度为 RSA-2048、RSA-4096

或者 ECC-256（NIST P-256）。

#### 1.4.1.2 CFCA OV SSL 全球服务器证书

CFCA OV SSL 全球服务器证书包含通配符证书、多域名证书、单域名证书类型。该类证书适合用于在订户浏览器与 Web 服务器之间建立安全通道，实现数据信息在客户端与服务器之间的加密传输，防止数据信息的泄露。

CFCA OV SSL 服务器证书由 CFCA OV OCA、CFCA OV RSA OCA G2、CFCA OV ECC OCA G2 签发 SHA256 证书，密钥长度为 RSA-2048、RSA-4096 或者 ECC-256（NIST P-256）。

#### 1.4.1.3 CFCA DV SSL 全球服务器证书

CFCA DV SSL 全球服务器证书包含单域名证书、多域名证书、通配符证书，该类证书适合用于在订户浏览器与 Web 服务器之间建立安全通道，实现数据信息在客户端与服务器之间的加密传输，防止数据信息的泄露。

CFCA DV SSL 全球服务器证书由 CFCA DV OCA、CFCA DV RSA OCA G2、CFCA DV ECC OCA G2 签发 SHA256 证书，密钥长度为 RSA-2048、RSA-4096 或者 ECC-256（NIST P-256）。

### 1.4.2 禁止的证书应用

CFCA 全球信任体系下的证书根据其类型在功能上有所限制，比如 CFCA EV SSL 服务器证书只能用于经过严格认证的 WEB 服务器。

各类证书的密钥用法在订户证书中的扩展项中进行了限制。然而基于证书

扩展项限制的有效性取决于应用软件，如果参与方不遵守相关约定，其对证书的应用超出本 CP/CPS 限定的应用范围，将不受 CFCA 的保护。

CFCA 全球信任体系下签发的证书不能在如下领域使用：任何与国家或地方法律、法规规定相违背的应用系统。

## 1.5 策略管理

### 1.5.1 策略文档管理机构

本 CP/CPS 的策略文档管理机构为 CFCA 业务管理部。当需要编写或修订本 CP/CPS 时，由业务管理部牵头组织相关人员成立“CP/CPS 编写组”，总经理也可以根据需要临时设立“CP/CPS 编写组”，并指定编写组负责人。

### 1.5.2 联系方式

如对本 CP/CPS 有任何疑问，请与 CFCA 业务管理部联系：

| | |
|---|---|
| 电话：010-80864610 | 传真：010-63555032 |
| 邮件：cps@cfca.com.cn | 地址：北京市西城区金融大街 37 号百盛北楼 8 层 |

如需要向 CFCA 提交证书问题报告，请在 CFCA 站点填写表单进行反馈：https://cloudpki.cfca.com.cn/cpr。

### 1.5.3 决定 CP/CPS 符合策略的机构

“CP/CPS 编写组”拟定初稿或修订稿后，交由公司“安全管理委员会”审议，“安委会”将负责评估 CP/CPS 是否符合相关要求，如果符合，将报总经理审批。总经理审批同意后，本 CP/CPS 方可对外发布，并自发布之日起 20 天

内向行业主管部门报备。

### 1.5.4 CP/CPS 批准程序

“CP/CPS 编写组”负责起草 CP/CPS 形成讨论稿，并征求公司领导和各部门负责人意见，经讨论、修改达成一致意见后形成送审稿。

“CP/CPS 编写组”负责将 CP/CPS 送审稿提交公司“安委会”审阅。在取得“安委会”评审意见后，“CP/CPS 编写组”据此进行修改并提交业务管理部，由业务管理部确定 CP/CPS 文本格式和版本号，形成定稿。

CP/CPS 定稿经公司各部门负责人及分管领导审阅后，报总经理审批。总经理审批同意后，方可对外发布 CP/CPS。发布形式应符合行业主管部门等相关主管部门要求，包括但不限于公司网站( https://www.cfca.com.cn )公布和向客户或合作对象书面提交。发布工作由业务管理部协调相关部门完成。

CP/CPS 的网上发布遵照《CFCA 网站管理办法》执行。自 CP/CPS 发布之日起,所有以各种形式对外提供的CP/CPS必须与网站公布的CP/CPS保持一致。业务管理部负责自发布之日起 20 天内向行业主管部门报备。

业务管理部定期对 CP/CPS 的内容进行审查,以发起修订申请。各部门也可根据业务发展变化需要及时向业务管理部提出修订申请。本 CP/CPS 也可以根据所遵循标准的要求，提出修订申请。

本 CP/CPS 至少每年修订一次。当修订内容具有重大变更时，CFCA 将按照与初次编写相同的流程进行；当修订内容变动较小时，由法律合规部修订完成后报各部门负责人及公司领导审阅，并经总经理审批同意后立即在公司网站上发布。每次修订完成后均需由业务管理部自发布之日起 20 日内向行业主管部

门报备。

## 1.6定义和缩写

### 1.6.1定义

| 项目 | 概念定义 |
| --- | --- |
| 电子认证服务机构 | 受订户信任的，负责创建和签发、管理公钥证书的权威机构，有时也可为订户创建密钥。 |
| 注册机构 | 面向证书订户，负责订户证书的申请、审批和证书管理工作。 |
| 数字证书 | 经CA数字签名包含数字证书使用者身份公开信息和公开密钥的电子文件。 |
| 证书吊销列表 | 由证书认证机构（CA）签发并发布的被吊销证书的列表 |
| 在线证书状态协议 | IETF颁布的用于检查数字证书状态的协议。 |
| 证书策略 | 一套命名的规则集，用以指明证书对一个特定团体和（或者）具有相同安全需求的应用类型的适用性。 |
| 电子认证业务规则 | 关于电子认证服务机构在签发、管理、吊销或更新证书（或更新证书中的密钥）过程中所采纳的业务实践的声明。 |
| 订户 | 申请证书的实体。 |
| 依赖方 | 依赖方是指信赖于证书所证明的基础信任关系并依此进行业务活动的个人或机构。 |
| 私钥 | 非对称密码算法中只能由拥有者使用的不公开密钥。 |
| 公钥 | 非对称密码算法中可以公开的密钥。 |
| 唯一甄别名 | 在数字证书的主体名称域中，用于唯一标识证书主体的X.500名称。此域需要填写反映证书主体真实身份的、具有实际意义的、与法律不冲突的内容。 |
| RFC5280 | RFC5280是X.509公钥基础设施证书和证书撤销列表的的配置文件。 |
| RFC6960 | RFC 6960:X.509互联网公钥基础设施在线证书状态协议-OCSP。 |
| X.509协议 | X.509 互联网公钥基础设施在线证书状态协议，X.509 是密码学里公钥证书的格式标准。 |
| X.500协议 | 数字证书的命名规则一般采用X.500格式。 |
| 网络视角 | 与多视角签发验证相关。指一个系统（如：云托管服务器实例）或一组网络组件（如：虚拟专用网络（VPN）及相应基础设施），用于发送与域名控制验证方法和 / 或 CAA 检查相关的出站互联网流量。网络视角（Network Perspective）的位置，由未封装的出站互联网流量通常首次传递至为该视角提供互联网连接的网络基础设施的节点决定。 |

| | |
|---|---|
| 主网络视角 | 证书颁发机构（CA）用于判定以下两项内容所采用的网络视角：1）该机构为申请域名或 IP 地址签发证书的权限；2）申请人对申请域名或 IP 地址所拥有的权限，以及/或对该域名或 IP 地址的授权或控制权。 |
| 多视角签发验证 | 在证书签发前，通过其他网络视角对主要网络视角（Primary Network Perspective）在域名验证（Domain Validation）和 CAA 检查过程中所做出的判定进行佐证的流程。 |
| 授权端口 | 以下端口之一：80（超文本传输协议，http）、443（超文本传输安全协议，https）、25（简单邮件传输协议，smtp）、22（安全外壳协议，ssh） |

## 1.6.2缩略词

| 项目 | 缩写 |
|---|---|
| ANSI | 美国国家标准协会（The American National Standards Institute） |
| CA | 电子认证服务机构（Certificate Authority） |
| RA | 注册机构(Registration Authority) |
| CRL | 证书吊销列表(Certificate Revocation List) |
| OCSP | 在线证书状态协议(Online Certificate Status Protocol) |
| CP | 证书策略(Certificate Policy） |
| CPS | 电子认证业务规则（Certificate practice Statement） |
| CSR | 证书签名请求（Certificate Signature Request） |
| IETF | 互联网工程任务组(The Internet Engineering Task Force) |
| DNS | 域名系统（Domain Name System） |
| FIPS | 联邦信息处理标准（Federal Information Processing Standards） |
| EV | 扩展验证/增强验证（Extended Validation） |
| DN | 唯一甄别名（Distinguished Name） |

## 1.6.3参考文献

1、http://csrc.nist.gov/publications/nistpubs/800-89/SP-800-89_November2006.pdf

互联网工程任务组（IETF）发布的 RFC3647 标准

2、CA/Browser 论坛（https://cabforum.org/）发布的以下最新版要求（自本 CP/CPS 发布前）：

（1） Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates

（2）Network and Certificate System Security Requirements

（3）Guidelines for the Issuance and Management of Extended Validation Certificates.

3、Mozilla Root Store Policy

4、Microsoft Trusted Root Program

5、AATL Technical Requirements

6、Apple Root Certificate Program

7、Chrome Root Program

8、360 Browser Root Certificate Program

9、Oracle Root Certificate

10、《Webtrust 安全审计规范》

### 1.6.4约定

本文中的关键词“必须”、“不得”、“要求”、“应”、“不应”、“应该”、“不应”、“推荐”、“可以”和“可选”根据 RFC 2119 进行解释。本文档所提日期的省略时间为北京时间 00:00:00（UTC+8）。

# 2 信息发布与信息管理

## 2.1信息库

CFCA 信息库面向订户及证书应用依赖方提供信息服务。CFCA 信息库包

括但不限于以下内容：证书、CRL、CP/CPS、证书服务协议、技术支持手册、CFCA 网站信息以及 CFCA 不定期发布的信息。

## 2.2 认证信息的发布

CFCA 的 CP/CPS 以及相关的技术支持信息等在 CFCA 网站 https://www.cfca.com.cn 上发布。本 CP/CPS 管理的证书依据主流根证书库要求，将证书日志记录于证书中的“证书透明列表（SCT 列表）”中进行公开。同时还提供在线证书状态查询、证书撤销查询服务等。

## 2.3 发布的时间或频率

CP/CPS 以及相关业务规则在完成 1.5.4 所述的批准流程后的 15 个工作日内发布到 CFCA 网站上，并可确保 7*24 小时可访问, CPS 至少每年更新一次；CRL 信息将在 24 小时内更新；订户有特殊要求的，将根据订户的需求，适当更新 CRL 发布的频率。CFCA 签发的 CRL 信息，根据需要，也可以人工方式实时发布。

## 2.4 信息库访问控制

CFCA 的安全访问控制机制确保只有经过授权的人员才能编写和修改信息库中的信息，CFCA 信息库中的信息以只读的方式对外提供查询和获取。

# 3 身份识别与鉴别

## 3.1 命名

### 3.1.1 名称类型

CFCA 全球信任体系下签发的证书根据证书类别的不同，签发的证书主体名字可能是域名、公网 IP 等，命名符合 X.500 定义的甄别名规范。

### 3.1.2 对名称意义化的要求

DN（Distinguished Name）：唯一甄别名，在数字证书的主体名称域中，用于唯一标识证书主体的 X.500 名称。此域需要填写反映证书主体真实身份的、具有实际意义的、与法律不冲突的内容。

EV SSL 全球服务器证书的甄别名称中的通用名只能是订户机构所拥有的域名，结合该订户的其他信息一起被鉴别和认证。

OV SSL 全球服务器证书的甄别名称中的通用名可以是订户所拥有的域名或者公网 IP，结合该订户的其他信息一起被鉴别和认证。

DV SSL 全球服务器证书的甄别名称中的通用名可以是订户所拥有的域名或者公网 IP，结合该订户的其他信息一起被鉴别和认证。

### 3.1.3 订户的匿名或伪名

使用匿名的订户提交的证书申请材料不符合 CFCA 的审核要求，将无法通过审核，也无法获得证书和服务。

使用伪名或伪造材料申请的证书无效，一经证实立即予以吊销。

### 3.1.4解释不同名称形式的规则

DN 的命名规则由 CFCA 定义，详见本 CP/CPS 7.1.4 的说明。

### 3.1.5名称的唯一性

在 CFCA 全球信任体系中，不同订户的证书的主体甄别名不能相同，且必须是唯一的。但对于同一订户，可以用其唯一的主体甄别名为其签发多张证书。当证书申请中出现不同订户存在相同名称时，遵循先申请者优先使用，后申请者增加附加识别信息予以区别的原则。

### 3.1.6商标的识别、鉴别和角色

CFCA 签发的证书不包含任何商标或者可能对其他机构构成侵权的信息，CFCA 颁发证书时不验证申请人是否使用商标或处于商标纠纷中，当发生有关纠纷时，CFCA 有权拒绝申请并吊销任何已发放的证书。

## 3.2初始身份确认

### 3.2.1证明拥有私钥的方法

订户必须证明持有与所注册公钥相对应的私钥，证明方法包括：pkcs#10、其他与此相当的密钥标识方法，或者 CA 机构接受的其他证明方式。CFCA 在为订户签发证书前，系统将自动使用订户的公钥验证其私钥签名的有效性和申请数据的完整性，以此来判断订户拥有私钥。

## 3.2.2机构身份的鉴别

### 3.2.2.1 机构身份的鉴别

机构订户在申请证书时，将进行严格的身份鉴别，如通过查询可信数据库验证其真实性、鉴别申请者提交的身份材料以及其他可以获得申请者明确的身份信息的方式等。机构订户的证书申请表上有申请者本身或被充分授权的证书申请者代表的签字（公章）表示接受证书申请的有关条款，并承担相应的责任。

对于包含组织身份信息的所有证书，CFCA 将验证组织的名称和注册经营地址，CFCA 可根据组织所申请的证书类别的不同，执行不同的身份鉴别方式，所使用的鉴别方式参考 CA/Browser 论坛的 BR 以及 EVG。CFCA 可以选择以下一项或多项来验证组织的身份和地址信息：

（1）通过以下合格的独立或政府信息来源，如公司/组织 注册中心的公开记录：

- 全国组织机构统一社会信用代码数据服务中心
- 国家企业信用信息公示系统
- 中华人民共和国商务部
- 企查查企业信息查询系统
- 天眼查企业信息查询系统
- ICP/IP 地址/域名信息备案管理系统

（2）通过政府机构签发的有效文件（包括但不限于工商营业执照，事业单位法人证书、统一社会信用代码证书等）或通过签发有效文件的权威第三方数据库以确认组织是真实存在的、合法的实体。

（3）通过可信的第三方数据库获取组织的地址及联系方式，以电话，电子邮件、邮政信函等方式与机构进行联络，以确认申请者所提供的信息的真实性。

（4）通过有执业资格的律师、会计师等出具的证明函件来验证信息。

（5）通过物业账单、银行对账单，政府签发的税单或其他 CFCA 认可的验证方式来确认机构的地址信息。

（6）委托第三方对机构进行调查，或要求申请者提供額外的信息及证明材料。此外，必要时，CFCA 还可以设定其它所需要的鉴别方式和资料。申请者有义务保证申请材料的真实有效，并承担与此相关的法律责任。

CFCA 建立和维护证书高风险申请人列表，在接受证书申请时会查询该列表，对于列表中出现的申请人，CA 机构将拒绝其申请。

#### 3.2.2.2 DBA/商业名称的鉴别

不适用。

#### 3.2.2.3 国家的鉴别

若证书主题项包含国家字段，CFCA 将通过 3.2.2 章节中申请者提供的机构证明信息进行所在国家的鉴别。

#### 3.2.2.4 域名的确认和鉴别

用户在申请 SSL 证书时，CFCA 需要验证申请者对所申请证书中域名的控制权，此验证过程由 CFCA 执行，不会委托给第三方。CFCA 不支持最右端为.onion 的域名的验证，且不提供该证书的签发。CFCA 会维护每个域名的验

证记录，包括使用了哪种验证方法以及对应的 BR 版本号。

#### 3.2.2.4.1 验证申请人为域名联系人

CFCA 不支持此方法。

#### 3.2.2.4.2 向域联系人发送电子邮件、传真、短信或邮政信件

CFCA 不支持此方法。

#### 3.2.2.4.3 域联系人电话联系

CFCA 不支持此方法。

#### 3.2.2.4.4 构造电子邮件到域联系人

按照基本要求第 3.2.2.4.4 节中的定义，构造电子邮件至域联系人。通过以下方式使用构建的电子邮件地址直接与域联系人通信，确认申请人对请求的 FQDN 的控制：

1、将电子邮件发送到一个或多个通过使用“admin”、“administrator”、“webmaster”、“hostmaster”或“postmaster”作为邮件地址部分，后跟符号（“@”），再后跟待验证的域名。

2、在电子邮件中包含一个随机值。

3、让申请人向 CFCA 的服务器提交（通过单击或其他方式）随机值以确认接收和授权。

唯一的随机值由 CFCA 生成，并在生成之日起有效期不超过 30 天。此验

证方式同时适用于通配符域名的验证。

#### 3.2.2.4.5 域名授权文件

CFCA 不支持此方法。

#### 3.2.2.4.6 商定的网站变更

CFCA 不支持此方法。

#### 3.2.2.4.7 DNS 变更

按照基本要求第 3.2.2.4.7 节中的定义，订户通过为待验证域名解析指定的带随机值的 TXT 或 CNAME 记录，CFCA 能够查询到指定记录即可完成域名所有权验证。

唯一的随机值由 CFCA 生成，并在生成之日起有效期不超过 30 天。

CFCA 采用本方法进行验证时，将依照第 3.2.2.9 节规定的多视角签发验证（Multi-Perspective Issuance Corroboration）执行操作。某一网络视角（Network Perspective）若要具备佐证效力，必须与主要网络视角（Primary Network Perspective）观测到相同的随机值（Random Value）。

若域名通过此方式完成控制权验证，CFCA 可以为此域名以及以此域名结尾的下级域名签发证书，此验证方式同时适用于通配符域名的验证。

#### 3.2.2.4.8 IP 地址

CFCA 不支持此方法。

#### 3.2.2.4.9 测试证书

CFCA 不支持此方法。

#### 3.2.2.4.10 使用随机数

CFCA 不支持此方法。

#### 3.2.2.4.11 任何其他方法

CFCA 不支持此方法。

#### 3.2.2.4.12 验证申请人为域名联系人

CFCA 不支持此方法。

#### 3.2.2.4.13 向 DNS CAA 联系人发送电子邮件

CFCA 不支持此方法。

#### 3.2.2.4.14 向 DNS TXT 联系人发送电子邮件

按照基本要求第 3.2.2.4.14 节中的定义，CFCA 将发送验证邮件到通过 DNS 查询到的"_validation-contactemail" TXT 解析的域名联系人邮箱。验证邮件中会包含一个唯一的随机值，订户收到验证邮件后，访问带随机值的验证链接，点击批准后即可完成域名所有权验证。

CFCA 采用本方法进行验证时，将依照第 3.2.2.9 节规定的多视角签发验证（Multi-Perspective Issuance Corroboration）执行操作。某一网络视角（Network

Perspective）若要具备佐证效力，必须与主要网络视角（Primary Network Perspective）观测到用于域名验证（Domain Validation）的同一选定联系地址。

唯一的随机值由 CFCA 生成，并在生成之日起有效期不超过 30 天。若域名通过此方式完成控制权验证，CFCA 可以为此域名以及以此域名结尾的下级域名签发证书，此验证方式同时适用于通配符域名的验证。

#### 3.2.2.4.15 电话验证域名联系人

CFCA 不支持此方法。

#### 3.2.2.4.16 向 DNS TXT 中电话联系人进行电话联系

CFCA 不支持此方法。

#### 3.2.2.4.17 向 DNS CAA 中电话联系人进行电话联系

CFCA 不支持此方法。

#### 3.2.2.4.18 商定的网站变更 V2

按照基本要求第 3.2.2.4.18 节中的定义，订户通过在待验证域名站点指定目录/.well-known/pki-validation/下放置指定的验证文件和随机验证值，CFCA 通过 HTTP/HTTPS 协议的授权端口能够成功访问到指定的验证内容即可完成域名所有权验证。

唯一的随机值由 CFCA 生成，并在生成之日起有效期不超过 30 天。若域名通过此方式完成控制权验证，CFCA 仅可为此域名签发证书。此验证方式不

适用于通配符域名的验证，CFCA 支持 http 协议层发起的状态码为 301、302 的重定向请求验证，重定向后的地址必须和验证域名一致，可以采用 http 或者 https 方式，且端口必须是授权端口。

CFCA 采用本方法进行验证时，将依照第 3.2.2.9 节规定的多视角签发验证（Multi-Perspective Issuance Corroboration）执行操作。某一网络视角（Network Perspective）若要具备佐证效力，必须与主要网络视角（Primary Network Perspective）观测到相同的随机值（Random Value）。

#### 3.2.2.4.19 使用 ACME 方式的网站变更

CFCA 不支持此方法。

#### 3.2.2.4.20 使用 TLS 的 ALPN 扩展

CFCA 不支持此方法。

#### 3.2.2.4.21 标有账户标识符的域名系统标签 - ACME

CFCA 不支持此方法。

### 3.2.2.5 IP 地址的确认和鉴别

CFCA 接受订户使用公有 IP 申请 SSL 证书，不为 IP 签发域名型和增强型证书。用于申请证书的 IP 需符合 IANA 规范且不可为保留 IP。CFCA 会维护每个 IP 的验证记录，包括使用了哪种验证方法以及对应的 BR 版本号。

#### 3.2.2.5.1 商定的网站变更

按照基本要求第 3.2.2.5.1 节中的定义，订户通过在待验证 IP 站点指定目录/.well-known/pki-validation/下放置指定的验证文件和随机验证值。CFCA 通过 HTTP/HTTPS 协议的授权端口能够成功访问到指定的验证内容即可完成域名所有权验证。唯一的随机值由 CFCA 生成，并在生成之日起有效期不超过 30 天。

CFCA 采用本方法进行验证时，将依照第 3.2.2.9 节规定的多视角签发验证（Multi-Perspective Issuance Corroboration）执行操作。某一网络视角（Network Perspective）若要具备佐证效力，必须与主要网络视角（Primary Network Perspective）观测到相同的随机值（Random Value）。

#### 3.2.2.5.2 向 IP 地联系人发送电子邮件传真、短信或邮政信件

CFCA 不支持此方法。

#### 3.2.2.5.3 反向地址查找

CFCA 不支持此方法。

#### 3.2.2.5.4 任何其他方法

CFCA 不支持此方法。

#### 3.2.2.5.5 电话联系 IP 地址联系方式

CFCA 不支持此方法。

#### 3.2.2.5.6 IP 地址的 ACME“http-01”方法

CFCA 不支持此方法。

#### 3.2.2.5.7 IP 地址的 ACME“tls-alpn-01”方法

CFCA 不支持此方法。

### 3.2.2.6 通配符域名的确认和鉴别

CFCA 对通配符右侧的域名进行控制权验证，验证规则遵循本 CP/CPS 第 3.2.2.4 节中的规定。通配符域名右侧若为顶级域名或公共后缀，CFCA 则拒绝为其签发证书。CFCA 不为通配符签发 EV 证书。

### 3.2.2.7 数据源的准确性

CFCA 在鉴别过程中使用的数据源会在官网中公布，在将任何数据源作为可靠数据源之前，CFCA 会对数据源的可靠性、准确性、防篡改及防伪造能力进行评估。并遵循 CA/B 论坛对数据源的要求考虑以下因素：

1、所提供信息的年限。

2、信息源的更新频率。

3、数据供应商及数据收集的目的。

4、数据的可公开访问性及可用性。

5、数据伪造和篡改的难度。

#### 3.2.2.8 认证机构授权记录

CFCA 关于 CAA 记录的策略见第 4.2 节。

#### 3.2.2.9 多视角签发验证

多视角签发确证机制旨在证书签发前，通过多个远程网络视角，对主网络视角所做出的判定（即域名验证通过/失败、CAA 权限允许/禁止）进行确证。该流程能够增强对特定前缀的边界网关协议（BGP）攻击或劫持的防护能力。

CFCA 在针对以下两项要求执行多视角签发确证时，会使用同一组网络视角：1）域名授权或控制权；2）CAA 记录检查。

所依赖的网络视角反馈的信息集合，必须为证书颁发机构（CA）提供必要信息，使其能够明确评估：

- 按第 3.2.2.4 节和第 3.2.2.5 节中规定的所依赖验证方法的要求，是否存在预期的 1）随机值、2）请求令牌、3）IP 地址或 4）联系地址；
- 按第 3.2.2.8 节的规定，证书颁发机构对所请求域名的签发权限。

第 3.2.2.4 节和第 3.2.2.5 节阐述了需要使用多视角签发确证的验证方法，以及网络视角如何确证主网络视角所做出的判定结果。

CFCA 在通过后续网络视角执行验证时，不会重复使用或缓存从某一网络视角获取的结果或信息（例如，不同的网络视角不能依赖共享的 DNS 缓存，以防止控制某一网络视角流量的攻击者对其他网络视角使用的 DNS 缓存进行投毒）。为网络视角提供互联网连接的网络基础设施，其管理方可能与提供运行该网络视角所需计算服务的组织为同一机构。远程网络视角与证书颁发机构之间的所有通信，均通过基于现代协议（如 HTTPS）的经过认证和加密的通道进

行。

网络视角可以使用与其非共址的递归 DNS 解析器。但网络视角所使用的 DNS 解析器，必须位于该网络视角所依赖的同一区域互联网注册管理机构服务区域内。此外，在一次多视角签发确证尝试中使用的任意一对 DNS 解析器，其直线距离必须至少为 500 公里。DNS 解析器的位置，以未封装的出站 DNS 查询通常首次移交至为该 DNS 解析器提供互联网连接的网络基础设施的地点为准。

CFCA 可以立即使用相同的验证方法或替代方法，重新尝试多视角签发确证。在重新尝试多视角签发确证时，CFCA 不依赖先前尝试中的确证结果。对于在任何时间段内可执行的最大验证尝试次数，没有相关规定。

法定人数要求表描述了与多视角签发确证相关的法定人数要求。当多个网络视角之间的直线距离至少为 500 公里时，它们被视为不同的网络视角。当远程网络视角与主网络视角以及法定人数中其他网络视角均不同时，它们被视为“远程”网络视角。

CFCA 可以重复使用 CAA 记录法定人数合规性的确证证据，最长使用期限为 398 天。向某一域名签发证书后，对于来自同一申请人的后续证书请求中涉及的相同域名及其子域名，远程网络视角在最长 398 天内可以省略对 CAA 记录的检索和处理。

法定人数要求表：

| 使用的不同远程网络视角数量 | 允许的未确证数量 |
| --- | --- |
| 2 - 5 | 1 |
| 6 及以上 | 2 |

CFCA 用于执行多视角签发确证的远程网络视角，其互联网连接依赖于相关网络（如互联网服务提供商或云服务提供商网络），这些网络需实施相应措施，以缓解全球互联网路由系统中发生的 BGP 路由事件。

### 3.2.3个人身份的鉴别

如果申请者的身份是自然人，CFCA 将会审核其姓名、地址以及证书申请的真实性等相关必要信息。对于个人身份证书，CFCA 会根据个人所申请的证书类别的不同，执行不同的身份鉴别方式，一般而言，证书类别越高，安全等级越高，鉴别方式越严格，鉴别内容越全面。

申请者需要证明其对请求中包含的某些身份属性有控制权，例如其包含在证书请求中证书涉及的电子邮件地址或域名。申请者还可能被要求提交有效的政府签发的带照片的证件（如居民身份证、护照、驾驶证，军官证或其他同等证件）的清晰副本。CFCA 会验证证件的副本是否与所请求的名称匹配，以及其他相关信息是否正确。

CFCA 通过以下一种或多种方式来鉴别和验证：

1、采用发送相关校验码电子邮件或通过电话、手机短信等其他可靠的方式来鉴别和验证申请者证书请求的真实性。CFCA 不确认、不担保所签发的证书中除验证信息以外的其他身份信息是真实的、可靠的、属于申请者本人的。

2、检查申请者所提交的证件副本是否有任何篡改或伪造的痕迹，必要时通过查询权威第三方数据库等可靠的方式对申请者提供的身份信息进行核实验证，以确保申请者所提供的信息与核查结果一致。

3、通过物业费账单、银行卡对账单或信用卡账单等核实申请者的地址或直

接依赖政府签发的身份证明文件来确认地址。

4、当申请信息包含组织信息时，可要求申请者提交任职证明文件、或查询第三方数据库、或发送确认电子邮件等方式来确认该组织是否存在，以及申请者是否是该组织成员。

此外，必要时，CFCA 还可以设定其它所需要的鉴别方式和资料。申请者有义务保证申请材料的真实有效，并承担与此相关的法律责任。对于 CFCA 签发的订户证书，CFCA 会建立评估标准用于识别存在潜在高风险欺诈情况的证书请求。对于被识别为“高风险”的证书请求，CFCA 可直接予以拒绝。

### 3.2.4 没有验证的订户信息

CFCA 签发的证书信息没有未经过验证的信息。

### 3.2.5 授权确认

当机构订户授权申请代表人办理证书业务时，CFCA 会使用章节 3.2.3 中所列的来源去获取可靠的通讯方式，以此验证申请代表人申请证书的真实性。

CFCA 可以直接与申请代表人确定证书申请的真实性，也可以与申请者组织内拥有权威的部门进行确认，例如申请者主要业务办公室，公司办公室，人力资源办公室，信息技术办公室或者 CFCA 认为合适的其他部门。

CFCA 也可以允许申请代表人提供授权信、雇佣证明或任何同等方式来验证其属于上述机构以及其代表行为被该机构授权。此外，CFCA 允许申请者指定独立个人来申请证书。若申请者以书面形式指定了可以进行证书申请的独立个人，则 CFCA 不接受任何超出该授权的证书请求。在收到申请者已核实的书

面请求时，CFCA 应向申请者提供其已授权人员的清单。

### 3.2.6 互操作准则

对于申请 CFCA 全球信任体系下的 EV SSL 证书、OV SSL 证书、DV SSL 证书，CFCA 承担对订户身份的鉴别职能，暂不委托其他机构行使此职责。

## 3.3 密钥更新请求的标识与鉴别

### 3.3.1 常规密钥更新的标识与鉴别

**1、 证书补发**

（1）订户证书（文件）丢失或损坏，例如存放证书的介质损坏。

（2）订户认为原有证书和密钥不安全（例如订户怀疑证书被盗用或密钥受到了攻击）。

（3）其他经 CFCA 认可的原因。

在证书初次发放后的十二个月内需进行重新申请，且该信息未发生变化，订户无需提交机构身份验证材料，CFCA 仅通过订户初次申请时的信息进行身份验证即可，但需要进行域名验证。同时，订户需要向 CFCA 重新提交 CSR 申请证书。超过十二个月后，则需对订户身份及域名所有权进行重新验证。验证流程及要求与初次申请相同。

**2、 证书换发**

换发是指在证书将要过期的一个月内，订户申请更新证书的操作。

在订户证书到期前的一个月内，CFCA 将通过适当的方式通知用户对证书进行换发操作。

EV SSL 证书、OV SSL 证书、DV SSL 证书换发时需要对订户身份进行重新验证。重新验证订户身份的验证流程及要求与初次申请相同。

EV SSL 证书、OV SSL 证书、DV SSL 证书换发操作成功时，旧证书将在一个月后吊销。已过期的证书换发不吊销老证书，按照新申请处理。新证书有效期将从证书换发之日起至原证书到期为止再另加一个证书有效周期（已经过期的证书换证，其有效期仅为新证书有效周期）。

### 3.3.2 吊销后密钥更新的标识与鉴别

证书吊销后的密钥更新等同于订户重新申请证书，其要求与 3.2.2 相同。

## 3.4 吊销请求的标识与鉴别

证书吊销请求的标识与鉴别流程见本 CP/CPS 的 4.9.3。

# 4 证书生命周期操作要求

## 4.1 证书申请

### 4.1.1 证书申请实体

任何实体需要使用 CFCA 全球信任体系下签发的证书时，均可向 CFCA 提出证书申请，其应对向 CFCA 提供的任何数据负责。

### 4.1.2 注册过程与责任

**1、注册过程**

在 CFCA 颁发证书之前，申请人应向 CFCA 提交资料包括但不限于：

（1）提交证书申请。

（2）生成密钥对提供密钥对的公钥(经签名的 CSR)。

（3）向 CFCA 提供 CSR。

（4）同意适用的订户协议。

（5）支付任何使用的费用。

**2、责任**

（1）申请者应事先了解订户协议、本 CP/CPS 等文件约定的事项，特别是其中关于证书适用范围、权利、义务和担保的相关内容。

（2）订户有责任向 CFCA 提供真实、完整和准确的证书申请信息和资料。

（3）注册机构有责任对订户提供的证书申请信息和身份证明材料进行检查和审核。

## 4.2 证书申请处理

### 4.2.1 执行身份识别与鉴别功能

当 CFCA 接收到订户的证书申请后,CFCA 审核团队会按本 CP/CPS 第 3.2 章节的要求，对订户的身份进行识别与鉴别，其处理流程为：

1、CFCA 处理证书申请至少需要设置 3 个可信角色：信息收集、信息验证、签发证书。

其中信息收集、信息验证可以由同一人完成；但签发证书人员需要与信息收集、信息验证职责分离。

2、对于证书申请处理，签发证书人员需对申请机构信息做最终审核。

（1）对所有用以验证申请机构证书申请的信息和文件进行复核，查找冲突的信息或需要进一步验证的信息。

（2）如复核人提出的问题确实需要得到进一步验证，CFCA 必须从申请机构、协议签署人、申请审批人或其他合格的独立信息来源取得进一步验证的资料或证据。

（3）CFCA 必须保证已收集的与证书申请相关的信息和资料，足以确保签发的证书不包含 CFCA 已知或应发现的错误信息，否则 CFCA 将会拒绝证书的申请并通知申请机构。

（4）如果部分或所有的身份验证资料内容使用语言不是 CFCA 的官方语言，那么 CFCA 将会使用经过适当的培训、具备足够的经验和判断能力的人员完成最终的交叉审核和尽职调查。CA 通过以下方法执行交叉审核与尽职调查。

①依赖翻译的材料内容。

②依赖拥有此语言能力的代理机构完成此步骤，CFCA 复核代理机构的检查结果，并且复核证书标准中的 CFCA 自我审核要求。

（5） CFCA 会根据以往因被怀疑或鉴别为网络钓鱼或具有其他诈骗用途而被拒绝证书请求或撤销的证书，建立和维护 SSL,证书高风险数据库列表，在接受证书申请时将会查询该列表信息,对于列表中出现的订户，CFCA 有权拒绝证书申请请求或执行额外的验证。

（6）CFCA 会对待签发证书主题别名扩展项中的每一个 DNS Name 做 CAA 记录检查，并按照 4.2.4 中的检查方法和结果判定是否批准该证书申请。

（7）申请人信息必须包括但不限于至少一个将被包含在证书的 subjectAltName 扩展中的完全合格域名或 IP 地址。

（8）第 6.3.2 节已明确定义订户证书有效期上限。CFCA 可在下列期限内复用先前验证所用之文件、数据或验证结果，前提为：

- 数据来源须符合第 3.2 节所列来源；
- 数据或验证完成日期距本次证书签发日不超过下表期限。

主体身份信息验证数据复用期限

| 证书签发日期 | 最大数据复用期限 |
| --- | --- |
| 2026 年 3 月 15 前后签发 | 825 天 |
| 2026 年 3 月 15 日后签发 | 398 天 |

对于根据第 3.2.2.4 节和第 3.2.2.5 节进行的域名和 IP 地址验证，所使用的任何数据、文件或已完成的验证结果必须是在签发证书前的最大天数内获取的，具体如下表所示：

域名和 IP 地址验证数据复用期限

| 证书签发日期在此及之后 | 证书签发日期在此之前 | 最大复用期限 |
| --- | --- | --- |
| | 2026 年 3 月 15 日 | 398 天 |
| 2026 年 3 月 15 日 | 2027 年 3 月 15 日 | 200 天 |
| 2027 年 3 月 15 日 | 2029 年 3 月 15 日 | 100 天 |
| 2029 年 3 月 15 日 | | 10 天 |

## 4.2.2 证书申请批准和拒绝

CFCA 按照本 CP/CPS 第 3.2.2 的要求对订户提交的申请材料及其身份信息进行鉴别，经鉴别符合要求后，将批准申请。若鉴别未通过，CFCA 将拒绝其申请，及时通知申请者并告知拒绝原因。

CFCA 成功完成了证书申请所必需的确认步骤后,通过签发正式证书来批准证书申请。

1、证书申请的批准：

如果符合下述条件，CFCA 可以批准证书申请:

（1）该申请完全满足 CP/CPS 第 3.2 章关于订户身份的识别和鉴别的规定。

（2）订户接受或者没有反对订户协议的内容和要求。

（3）订户已经按照规定支付了相应的费用，另有协议规定的情况除外。

2、证书申请的拒绝：

如果发生下列情形，CFCA 有权拒绝证书申请:

（1）该申请不符合本 CP/CPS 第 3.2 章节关于订户身份识别和鉴别的规定。

（2）订户不能根据要求提供所需的身份证明材料。

（3）订户反对或者不能接受订户协议的有关内容和要求。

（4）订户没有或者不能够按照规定支付相应的费用。

（5）申请的证书含有 ICANN(The Internet Corporation for Assigned Names and Numbers)考虑中的新 gTLD(顶级域名)。

（6）订户证书的使用途径不符合其所在地的法律法规。

（7）CFCA 认为批准该申请将会对 CFCA 带来争议、法律纠纷或者损失。

（8）提交申请的公钥长度、算法或其他存在不安全因素。

（9）CFCA 拒绝颁发包含内部名称或预留 IP 地址的证书，因为这些名称不能根据第 3.2.2.2.4 或第 3.2.2.5 节进行验证。

### 4.2.3 处理证书申请的时间

CFCA 将在合理的时间内完成证书申请处理。在申请者提交的资料齐全且审核通过的情况下，1-3 个工作日处理完成。EV SSL 全球服务器证书处理证书申请时间不超过 5 个工作日，特殊情况最长不超过 10 个工作日。

### 4.2.4 认证机构授权记录（CAA）

CFCA 遵循 CA/B Forum BR 要求，对证书申请中的所有主题名称和备用名称中的域名进行 DNS CAA 记录检查。

CFCA 可以在任何时间进行 DNS CAA 记录检查。

CFCA 将在查询 CAA 记录的有效期（有效期以 CAA 记录的生存时间或 8 小时的较大值为准）内，向证书申请者发放证书。若超过 CAA 记录的有效期，将重新进行 CAA 检查。

CFCA 按照 RFC 8659 中的规定处理 CAA 记录中的"issue" ,"issuewild" , "iodef"属性标签。

CFCA 在处理 CAA 记录中的属性标签时，不会对"iodef"属性标签的内容进行操作。

CFCA 尊重关键标签，但遇到关键标签中设置了无法识别的属性时，将拒绝为其签发证书。

CAA 记录中若存在"issue" ,"issuewild" 标签，且"issue" ,"issuewild" 不包含"cfca.com.cn"，CFCA 将拒绝为其签发相应证书。

CFCA 采用本方法进行验证时，将依照第 3.2.2.9 节规定的多视角签发验证（Multi-Perspective Issuance Corroboration）执行操作。某一网络视角（Network

Perspective）若要具备佐证效力，无论两个视角的响应在字节层面是否完全一致，远程网络视角的 CAA 检查响应都必须被解读为允许签发。此外，若两个视角中任意一个或两个都出现了本节所定义的可接受的 CAA 记录查询失败情况，CFCA 也可将远程网络视角的响应视为具有确证效力。

在以下 CAA 查询失败情况下，CFCA 可为用户颁发证书：

1、 CAA 查询失败不是由 CFCA 的基础设施引起。

2、CFCA 至少重试过一次查询。

3、域名所在域不存在指向 ICANN 根域的 DNSSEC 验证链。

## 4.3 证书签发

### 4.3.1 证书签发中电子认证服务机构的行为

在订户申请通过鉴别后，RA 系统操作员录入订户申请信息，并提交 RA 系统审核员审核；RA 系统审核员审核通过后，向 CA 系统提交申请；CA 系统向 RA 系统返回证书，由 CA 以安全的形式将证书反馈给订户。

#### 4.3.1.1 根 CA 证书颁发的手动授权

根 CA 的证书颁发过程由 CFCA 授权的个体(CA 系统操作员、系统管理员或 PKI 管理员)手动发出明确的指令，以便根 CA 执行证书签名操作。

#### 4.3.1.2 使用 Linting 工具检测待签名证书内容

对于 SSL 服务器证书，在证书签名之前，对证书进行 linting 检测并结合错误信息进行人工复核，以防止签发违反 BR 要求。

#### 4.3.1.3 使用 Linting 工具检测已签发的证书

CFCA 使用 linting 工具检测所签发的 SSL 证书。

### 4.3.2 电子认证服务机构和注册机构对订户的通告

无论是拒绝还是批准订户的证书申请，CFCA 有义务告知订户申请结果。CFCA 会以电话、电子邮件或其他方式对订户进行通告。

## 4.4 证书接受

### 4.4.1 构成接受证书的行为

订户全权负责在订户的计算机或硬件安全模块上安装已签发的证书。

订户被认为接受已签发的证书的行为包括但不仅限于:

（1）订户自行访问专门的 CFCA 证书服务网站，将证书下载至数字证书载体中，并下载完毕。

（2）CFCA 在订户允许下，代替订户下载证书，并把证书通过安全载体发送给订户。

（3）证书获取通知发送给订户后，订户通过该通知下载证书。

（4）订户接受了获得证书的方式，并且没有提出反对证书或者证书中的内容。

### 4.4.2 电子认证服务机构对证书的发布

对于最终订户证书，CFCA 将根据订户的意愿采取适当形式的发布；订户没有要求发布的，CFCA 将不发布最终订户证书。

### 4.4.3 电子认证服务机构对其他实体的通告

对于 CFCA 签发的证书，CFCA 不对其他实体进行主动通告，依赖方可以在信息库上自行查询。

## 4.5 密钥对和证书的使用

### 4.5.1 订户私钥和证书的使用

订户的私钥和证书应用于规定的、批准的用途（在本 CP/CPS1.4.1 节定义），订户在使用证书时必须遵守本 CP/CPS 的要求，妥善保存其私钥，采取合理的措施防止私钥遗失、泄露、被篡改。避免他人未经本人授权而使用本人证书情形的发生，否则其应用是不受保障的。

证书持有者只能在指定的应用范围内使用私钥和证书，证书持有者只有在接受了相关证书后才能使用对应的私钥，并且在证书到期或被吊销后，须停止使用该证书及对应的私钥。

### 4.5.2 依赖方对公钥和证书的使用

依赖方信赖 CFCA 全球信任体系签发的证书所证明的信任关系时需要：

1、获取并安装该证书对应的证书链。

2、在信赖证书所证明的信任关系前确认该证书为有效证书，包括：检查 CFCA 公布的最新 CRL，或者通过 CFCA 提供的 OCSP 服务确认该证书未被吊销；检查该证书路径中所有出现过的证书的可靠性；检查该证书的有效期；以及检查其他能够影响证书有效性的信息。

3、在信赖证书所证明的信任关系前确认该证书记载的内容与所要证明的内

容一致。

4、确认该签名对应的证书是依赖方信任的证书。

5、证书的用途适用于对应的签名。

6、使用证书上的公钥验证签名。

7、考虑本 CP/CPS 或其它地方规定的其它信息。

以上条件不满足的话，依赖方有责任拒绝签名信息。

## 4.6 证书更新

### 4.6.1 证书更新的情形

对于 CFCA 签发的订户证书，证书到期前 30 日(含)起可以进行证书更新，在证书到期前 30 日(含)起，CFCA 会通过邮件通知的方式通知订户更新证书。

若订户提交证书更新请求时不变更证书主体甄别名及相关身份信息，且原证书的验证时效未超过本 CP/CPS 第 4.2.1 章节规定的期限，则 CFCA 可以参照原证书核实的数据及证明文件来验证更新证书的信息。

若订户提交证书更新请求时需要变更部分证书信息或原证书的验证时效已超过本 CP/CPS 第 4.2.1 章节规定的期限，则 CFCA 将按照证书初次申请的流程及要求进行验证。

若订户原来证书已过期，再次申请证书时按证书初次申请的流程及要求进行验证。

### 4.6.2 请求证书更新的实体

请求证书更新的实体为已经申请过 CFCA 证书的订户或其他授权代表人

且其证书剩余有效期少于 30 日(含)。

所有持有 CFCA 签发的证书订户，包括个人、企业单位、事业单位、政府机构、社会团体、人民团体等各类组织机构等，在其证书的有效期即将到期前，均可以请求更新其持有的各类证书。

### 4.6.3 证书更新请求的处理

对于证书更新，其处理过程包括申请识别和鉴别、证书信息验证及签发证书。

1、对于申请的识别和鉴别须基于以下几个方面:

（1）订户的原证书存在并且由 CFCA 所签发。

（2）证书更新请求在许可期限内。

（3）订户需提交能够识别原证书的足够信息，如订户甄别名、证书序列号等。

2、对于证书信息验证的处理过程，CFCA 将按照本 CP/CPS 第 3.3.1 章节之规定进行处理;

3、CFCA 也可以根据订户证书更新的具体申请情况，选择按一般初次证书申请流程进行验证。

以上鉴别和验证全部通过后，CFCA 才可以批准签发证书。

### 4.6.4 颁发新证书时对订户的通告

同 CP/CPS 第 4.3.2 章节。

### 4.6.5构成接受更新证书的行为

同 CP/CPS 第 4.4.1 章节。

### 4.6.6CA 对更新证书的发布

同本 CP/CPS 第 4.4.2 章节。

### 4.6.7CA 对其他实体的通告

同本 CP/CPS 第 4.4.3 章节。

## 4.7证书密钥更新

证书密钥更新是指订户生成新密钥并申请为新公钥签发新证书。

### 4.7.1证书密钥更新的情形

当订户的证书出现下列情形时，订户可选择证书密钥更新服务:

1、当订户证书即将到期或已经到期时。

2、当订户证书密钥遭到损坏时。

3、当订户证实或怀疑其证书密钥不安全时。

4、当订户证书丢失或损失时。

5、订户需要增加域名(仅限于多域名 SSL/TLS 服务器证书)。

6、订户一张证书多处部署，需要使用不同的密钥对。

7、其它可能导致密钥更新的情形。

证书即将到期的订户，出于安全考虑，应尽量采取证书密钥更新，来获得

新的证书。

### 4.7.2 请求证书密钥更新的实体

请求证书密钥更新的实体为已经申请过 CFCA 证书且其证书未过期的订户或其他授权代表人。

所有持有 CFCA 签发的证书订户，包括个人、企业单位、事业单位、政府机构、社会团体、人民团体等各类组织机构等，均可以请求证书密钥更新服务。

### 4.7.3 证书密钥更新请求的处理

CFCA 对证书密钥更新请求的处理通过证书更新请求处理流程完成，参见本 CP/CPS 第 4.6.3 章节的描述。

### 4.7.4 颁发更新证书时对订户的通告

同本 CP/CPS 第 4.3.2 章节。

### 4.7.5 构成接受密钥更新证书的行为

同本 CP/CPS 第 4.4.1 章节。

### 4.7.6 电子认证服务机构对密钥更新证书的发布

同本 CP/CPS 第 4.4.2 章节。

### 4.7.7 电子认证服务机构对其他实体的通告

同本 CP/CPS 第 4.4.3 章节。

## 4.8 证书变更

CFCA 不提供证书变更服务。

### 4.8.1 证书变更的情形

不适用。

### 4.8.2 请求证书变更的实体

不适用。

### 4.8.3 证书变更请求的处理

不适用。

### 4.8.4 颁发新证书时对订户的通告

不适用。

### 4.8.5 构成接受变更证书的行为

不适用。

### 4.8.6 CA 对变更证书的发布

不适用。

### 4.8.7 CA 对其他实体的通告

不适用。

## 4.9 证书吊销和挂起

### 4.9.1 证书吊销的情形

#### 4.9.1.1 订户证书吊销的原因

订户证书吊销，将根据不同吊销原因，遵循以下要求。

若出现以下情况的一种或多种，CFCA 在 24 小时之内吊销证书：

（1）订户以书面形式请求吊销证书。

（2）订户通知 CFCA 最初的证书请求未得到授权且不能追溯到授权行为。

（3）CFCA 获得了证据，证明与证书公钥对应的订户私钥遭到了损害。

（4）CFCA 具有验证订户私钥泄露的方法，此类方法可根据公钥轻易计算私钥值（如 Debian 弱密钥，见 https://wiki.debian.org/SSLkeys），或者有明确的证据证明订户用来生成私钥的方法是有缺陷的。

（5）CFCA 获得证据，证书中所包含的域名或 IP 地址的控制权验证已不再可靠。

若出现以下情况的一种或多种，CFCA 宜在 24 小时内撤销证书，且必须在 5 天内吊销证书：

（1）CFCA 获悉证书不再符合 BR 第 6.1.5 节及第 6.1.6 节的相关要求。

（2）CFCA 获得了证书遭到误用的证据。

（3）CFCA 获悉订户违反了订户协议、CP/CPS 中的一项或多项重大义务。

（4）CFCA 获悉任何表明 FQDN 或 IP 地址或邮箱地址的使用不再被法律许可（例如，某法院或仲裁员已经撤销了域名注册人使用域名的权力，域名注册人与申请人的相关许可及服务协议被终止，或域名注册人未成功续期域名，或证书正式的邮箱地址不再被订户合法使用）。

（5）当 CA 有证据表明订户已丧失证书中域名的使用权，或订户未能更新其域名使用权。

（6）CA 获知通配符证书被用于验证具有欺诈误导性质的域名。

（7）CFCA 取得了合理证据表明或意识到订户证书中的重要信息内容已经变更。

（8）CA 正式签发时未能满足证书策略或证书标准中的要求和条件，或者证书中的任何信息不准确。

（9）CA 认定证书中所显示的信息为不准确或具有误导性；或者订户申请证书时，提供的资料不真实。

（10）CFCA 因某些原因停止业务，并且没有安排其他的 CA 提供证书吊销服务。

（11）当 CFCA 从事电子认证业务的资格被吊销后，CFCA 除继续维持 CRL/OCSP 信息库的情况外，将吊销或终结所有已签发的证书。

（12）CFCA 用于签发证书的 CA 证书私钥可能被泄露时，将根据应急预案吊销所有已签发的证书。

（13）CFCA 取得了合理证据表明或意识到订户已经被列在相关的黑名单中，或其经营地区被 CFCA 所在国家的监管机构禁止。

（14）证书的重要参数被国际国内主流标准认为有重大风险时。

（15）法律、行政法规规定的其他情形。

#### 4.9.1.2 中级 CA 证书吊销的原因

若出现以下情况中的一种或多种，CFCA 应在 7 天之内撤销中级 CA 证书：

（1）中级证书签发机构正式书面申请撤销。

（2）中级证书签发机构发现并通知 CFCA 初始证书请求未经过授权且不能追溯到授权行为。

（3）CFCA 获得了证据，证明与证书公钥对应的中级 CA 私钥到了损害，或不再符合 BR 第 6.1.5 节及第 6.1.6 节的相关要求。

（4）CFCA 获得了证书遭到误用的证据。

（5）CFCA 获悉中级证书的签发未能符合 BR 要求，或中级 CA 未能符合 CP/CPS。

（6）CFCA 认为任何出现在中级 CA 证书中的信息不准确、不真实或具有误导性。

（7）CFCA 由于任何原因停止运营，且未与另一家 CA 达成协议以提供证书撤销服务。

（8）CFCA 依据 BR 签发证书的权力失效，或被撤销或被终止，除非其继续维护 CRL/OCSP 信息库。

（9）本 CP/CPS 要求撤销中级 CA 证书。

（10）证书的技术内容或格式给应用软件供应商或依赖方带来了不可接受的风险（例如，CA/Browser 论坛可能确定不赞成使用的加密 / 签名算法或密钥大小带来不可接受的风险。

### 4.9.2请求证书吊销的实体

请求证书吊销的实体可为订户、RA、CFCA。此外，依赖方、应用软件提供商，其他的第三方可以提交证书问题报告，告知 CFCA 有合理理由撤销证书。已申请 CFCA 证书的订户可请求证书吊销。

### 4.9.3请求吊销的流程

吊销分为主动吊销和被动吊销。主动吊销是指由订户提出吊销申请，由 CFCA 审核通过后吊销证书的情形；被动吊销是指当 CFCA 确认订户违反证书应用规定、约定或订户主体已经消亡等情况发生时，采取吊销证书的手段以停止对该证书的证明，CFCA 也接受任何实体提供的举报材料。

#### 4.9.3.1 主动吊销

订户申请吊销证书前应指定并书面授权证书吊销申请代表，提供有效身份证明文件及证书吊销申请文件，并接受证书吊销申请的有关条款，同意承担相应的责任。

CFCA 7*24 接受订户证书吊销申请，并处理订户证书吊销请求。

CFCA 收到订户的吊销申请材料后，将查询订户需吊销的证书是否为 CFCA 所发放，证书是否在有效期内，吊销理由是否属实，若均通过则对证书进行吊销。

#### 4.9.3.2 被动吊销

当出现被动吊销的情形时，CFCA 将以适当形式通知订户，告知拟吊销的

证书内容、吊销原因、吊销操作时限等事项，在确认订户收到吊销通知且无异议后予以吊销。

### 4.9.4 吊销请求宽限期

在主动吊销的情形下，订户一旦发现需要吊销证书，应及时向 CFCA 提出吊销请求。

在被动吊销的情形下，订户在收到吊销通知后的 3 个工作日内可向 CFCA 提出申辩理由，CFCA 将会对申辩理由进行评估，若确认其理由正当则不予以吊销；若订户在 3 个工作日内未回复或回复无异议则 CFCA 将予以吊销。

### 4.9.5 CFCA 处理吊销请求的时限

在主动吊销的情形下，CFCA 收到吊销请求并审核完成后，24 小时内吊销证书。

在被动吊销的情形下，订户在收到吊销通知后的 3 个工作日内可向 CFCA 提出申辩理由，CFCA 将会对申辩理由进行评估，若确认其理由正当则不予以吊销；若订户在 3 个工作日内未回复或回复无异议，则 CFCA 将于 24 小时内予以吊销。

若出现章节 4.9.1 第一部分的情形时，CFCA 将会在 24 小时内完成证书撤销。

### 4.9.6 依赖方检查证书吊销的要求

依赖方在信任此证书前应检查证书的有效性，确认证书未被吊销。

### 4.9.7 CRL 发布频率

CFCA 针对不同系统签发的证书区别更新 CRL 信息，对于 CFCA EV OCA、CFCA OV OCA、CFCA DV OCA、CFCA EV RSA OCA G2、CFCA OV RSA OCA G2、CFCA DV RSA OCA G2、CFCA EV ECC OCA G2、CFCA OV ECC OCA G2、CFCA DV ECC OCA G2 系统，将在 24 小时内更新 CRL 列表；订户有特殊要求的，将根据订户的需求，适当更新 CRL 发布的频率。CFCA 签发的 CRL 信息，根据需要，也可以人工方式实时发布。

### 4.9.8 CRL 发布的最大滞后时间

CRL 发布的最大延迟时间不超过 24 小时。

### 4.9.9 在线证书状态查询的可用性

CFCA 提供 OCSP 查询服务，服务 7*24 小时可用。

信赖方是否进行在线状态查询完全取决于信赖方的安全要求。对于安全保障要求高并且完全依赖证书进行身份鉴别与授权的应用，信赖方在信赖一个证书前可通过证书状态在线查询系统检查该证书的状态。

证书或预证书签发后，可在 15 分钟内通过在线证书状态协议（OCSP）查询服务器证书的状态。

CFCA 会在下次更新（nextUpdate）前至少 8 小时提供更新后的 OCSP 响应，并且最迟在本次更新（thisUpdate）后的 4 天内。

对于从属证书颁发机构（Subordinate CA）证书的状态，CFCA 至少每 12 个月提供一次更新后的 OCSP 响应，且会在证书被吊销后的 24 小时内提供更新。

### 4.9.10 在线证书状态查询要求

CFCA 的 OCSP 响应符合 RFC6960 标准。

客户通过 http 协议访问 CFCA 的 OCSP 服务，CFCA 会对查询请求进行检查，检查的内容包括：

（1）验证是否强制请求签名

（2）用 CA 证书验证签名是否通过

（3）验证证书是否生效或者已经过期

（4）验证证书颁发者是否在信任证书列表内

OCSP 响应包含如下表所述基本域和内容

| 域 | 值或者值的限制 |
|---|---|
| 状态 | 响应状态，包括成功、请求格式错误、内部错误、稍候重试、请求没有签名和请求签名证书无授权，当状态为成功时必须包括以下各项。 |
| 版本 | V1 |
| 签名算法 | 签发 OCSP 的算法。SHA256RSA 算法签名。 |
| 颁发者 | 签发 OCSP 的实体。签发者公钥的数据摘要值和证书甄别名。 |
| 产生时间 | OCSP 响应的产生时间。 |
| 证书状态列表 | 包括请求中所查询的证书状态列表。每个证书状态包括证书标识、证书状态以及证书废止信息。 |
| 证书标识 | 包括数据摘要算法、证书甄别名数据摘要值、证书公钥数 |

| | |
|---|---|
| | 据摘要值和证书序列号。 |
| 证书状态 | 证书的最新状态，包括有效、吊销和未知。 |
| 证书废止信息 | 当返回证书状态为废止时包含废止时间和废止原因。 |

OCSP 的扩展信息与 RFC6960 一致。

CFCA 的 OCSP 信息的更新频率不超过 24 小时，OCSP 服务响应最大时间不超过 10 秒，OCSP 服务响应信息最大有效期不超过 7 天。

### 4.9.11 吊销信息的其他发布形式

证书吊销信息可以通过 CRL 或者 OCSP 服务获得。订户可通过证书扩展域中的 CRL 地址获得 CRL 信息。

### 4.9.12 对密钥遭受安全威胁的特别处理要求

当订户发现、或有充足的理由发现其密钥遭受安全威胁时，应及时提出证书吊销请求。

密钥泄露可通过以下方式之一来证明：

1. 将泄露的密钥移交给 CFCA，

2. 向名为“证明 CFCA 密钥泄露”的 CSR 提交，该 CSR 已使用泄露的密钥进行签名

本 CP/CPS 第 1.5.2 节描述了向 CFCA 通报密钥泄露的方法。

### 4.9.13 证书挂起

对于全球信任体系下颁发的证书，CFCA 目前暂不提供此业务。

### 4.9.14 请求证书挂起的实体

不适用。

### 4.9.15 请求证书挂起的流程

不适用。

### 4.9.16 挂起的期限限制

不适用。

## 4.10 证书状态服务

### 4.10.1 操作特征

证书状态可以通过 CFCA 提供的 CRL 和 OCSP 服务获得。

### 4.10.2 服务可用性

CFCA 提供 7*24 小时不间断证书状态查询服务。CFCA 运行并维护其 CRL 和 OCSP 功能，其资源足以在正常工作条件下提供 10 秒或更短的响应时间。

### 4.10.3 可选功能

不适用。

## 4.11 订购结束

以下两种情形将被视为订购结束：

1、 证书到期后即视为订购结束。

2、 证书吊销视为订购结束。

## 4.12 密钥生成、备份与恢复

为保证订户密钥的安全性，订户应在安全的环境下独立生成密钥对，并将生产的密钥通过加密等手段存储在安全的介质中，订户应及时备份密钥，并确保备份密钥的安全性，以防密钥丢失。在生成密钥对之后与安装服务器证书之前的时期内不应更改服务器的任何配置，以防密钥丢失。在密钥丢失或可能泄漏后，需及时申请密钥更新。

在订户委托其他可信服务商代替订户生成密钥对的情况下，应要求服务商承担相应的保密责任。

### 4.12.1 密钥生成、备份与恢复策略及实践

不适用。

### 4.12.2 会话密钥封装与恢复策略及实践

不适用。

# 5 认证机构设施、管理和操作控制

## 5.1 物理控制

系统的物理安全和环境安全是整个 CFCA 系统安全的基础，它包括基础设施的管理、周边环境的监控、区域访问控制、设备安全及灾难预防等各方面。

为保证 CFCA 系统物理环境的安全可靠，CFCA 系统被放置于安全稳固的建筑物内并具备独立的软硬件操作环境，充分考虑了水患、火灾、地震、电磁干扰与辐射、犯罪活动以及工业事故等的威胁。

### 5.1.1 场地位置与建筑

CFCA CA 系统的运营机房位于北京市海淀区中关村软件园区 22 号楼（中国银联北京信息中心楼内）内，进入机房须通过审核和多道门禁系统，机房电磁屏蔽效能满足 GJB5792-2006 标准“C”级要求。机房具备抗震、防火、防水、恒湿温控、独立供电、备用发电、门禁控制、视频监控等功能，可保证认证服务的连续性和可靠性。

监控记录文件包括对机房通道上的所有踪迹的记录。所有经 CFCA 授权的人员在限制区域活动都需要有 CFCA 人员的陪同。CFCA 授权的人员清单会提供给 CFCA 运行负责部门，以保证只有经授权的 CFCA 人员才能进入机房。对于要进入机房的 CFCA 的来访者，只有经过相应批准后，由 CFCA 授权的员工陪同才可进入。

所有 CFCA 授权的服务机构，包括注册机构、受理点等的证书服务系统也必须受到保护，确保只有经授权的员工才能进入该系统进行操作。CFCA 的管理员负责设置和检查注册机构、受理点管理员的权限。注册机构、受理点操作员的权限和责任在运作协议中也作出了规定。

#### 5.1.1.1 公共区

CFCA 场地的入口、配电在该区域，采用访问控制措施，需要使用门禁卡

或指纹鉴别才可进入。

#### 5.1.1.2 管理服务区

服务区是 CFCA 操作人员、管理人员的工作区，需要 2 名可信人员同时使用门禁卡和指纹鉴别才可以进入，人员进出服务区有日志记录。

#### 5.1.1.3 核心区

核心区是 CA 运营管理区域，此区域必须使用门禁卡和指纹鉴别才可以进入。同时，证书认证系统、加密设备等相关密码物品也存放在该区域，其中 CA 服务器、数据库系统、以及加密设备等相关密码物品位于核心区内的屏蔽机房内。屏蔽机房必须两名可信人员同时使用门禁卡和指纹鉴别才可以进入，确保在屏蔽区内单个人员无法完成敏感操作。在屏蔽区内有单独的缓冲区，防止在开启屏蔽门时，电磁波泄露发生。

### 5.1.2 物理访问

外来人员进入楼内，需经过中国银联北京信息中心、CFCA 两道的审核，进入 CFCA 办公区域要经过两道门禁系统，需要有 CFCA 工作人员陪同进入。

操作人员进入 CFCA 综合机房，须经过指纹认证加门禁授权卡身份认证，并有 24 小时视频监控设备进行监控。

操作人员进入安全区机房，须经过三道门禁系统，其中两道是双人指纹加门禁卡认证，一道是双人门禁卡认证，并且所有门禁的进出信息都会在监控室的安保系统中记录。

### 5.1.3 电力与空调

CFCA 机房采用 UPS 供电，由两组每组三台 UPS 线路供电，任何一台 UPS 出现故障，均能保证系统供电持续运行 30 分钟以上。为了保证系统的可靠运行，还备有柴油发电机，当外部供电中断时，能够继续对 UPS 实施供电。

CFCA 机房采用多台中央空调和新风设备，保证机房内温度和湿度达到国家标准（GBJ19-87《采暖通风与空气调节设计规范》、GB50174-93 《电子计算机机房设计规范》）。

### 5.1.4 水患防治

CFCA 有专门的技术措施防止、检测漏水的出现，并能够在出现漏水时最大程度地减小漏水对认证系统的影响。

### 5.1.5 火灾防护

CFCA 机房采用防火材料建设，安装有中央防火监控和自动气体消防系统，并通过了国家权威部门的消防功能验收，能有效地避免火灾威胁。

### 5.1.6 介质存储

对于存放重要数据的存储介质，CFCA 制订了专门的管理控制制度，以防止重要信息的泄露与人为故意产生的危害和破坏。

### 5.1.7 废物处理

敏感的文件资料（包括纸介质、光盘或软盘废物等）抛弃前要进行粉碎处

理；对于存储或传输信息的介质，在抛弃前要做不可读取处理；涉密介质在抛弃前要根据生产商的指导做归零处理。加密机等重要设备废弃根据加密机管理办法销毁。

### 5.1.8数据备份

目前 CFCA 已对核心数据建立同城数据备份机制。

CFCA 对关键数据、审计日志数据使用离线介质进行备份并运送到异地保存，保存设施满足 5.1.6 介质存储的描述。

1、系统备份:

CA 系统进行异地的系统备份，预防系统因为不定因素不能正常运行。在主系统不能正常运行时，备份系统将投入使用，继续提供认证服务。

2、数据备份:

CFCA 同时进行异地的数据备份。异地备份的操作在 CFCA 灾难恢复计划中进行规定。CFCA 异地数据备份介质安全要求都符合 CFCA 备份标准和程序。

## 5.2程序控制

### 5.2.1可信角色

CFCA 的可信角色包括：

安全管理人员

密钥与密码设备管理人员

加密设备操作人员

系统管理人员

人力资源管理人员

安全审计人员

证书录入人员

证书鉴别人员

CA 系统开发人员

客户服务人员

### 5.2.2 每项任务需要的人数

CFCA 制定了规范的策略，严格控制任务和职责的分割，对于最敏感的操作。例如：

1、屏蔽区场地访问：设置为 2 个可信人员进出模式。

2、鉴别、审核和签发证书：需要 2 个可信人员共同完成。

3、密钥和密码设备的操作和存放：需要 5 个可信人员中的 3 个共同完成。

4、CA 系统后台操作：需要 2 个可信人员共同完成。

5、重要系统数据操作和维护：需要至少 1 人操作，1 人监督记录。

CFCA 对于人员有明确的分工，贯彻互相牵制、互相监督的安全机制。

### 5.2.3 每个角色的识别与鉴别

CFCA 在雇佣一个可信角色之前将会按照本 CP/CPS 第 5.3.2 节的规定对其进行背景审查。

对于物理访问控制，CFCA 通过门禁磁卡、指纹识别鉴别不同人员，并确定相应的权限。

CFCA 使用数字认证和订户名/口令方式对可信角色进行识别与鉴别，系统将独立完整地记录所有操作行为。

### 5.2.4 需要职责分割的角色

要求职责分割的角色包括（但不限于）以下几种：

安全管理员、系统管理员、网络管理员、订户身份及信息审核人员、证书录入人员、证书鉴别人员。

## 5.3 人员控制

CFCA 及其注册机构应按照以下要求进行人员管理及控制。

### 5.3.1 资格、经历和无过失要求

成为 CFCA 可信角色的人员必须提供相关的背景、资历证明，并具有足以胜任其工作的相关经验，且没有相关的不良记录。

### 5.3.2 背景审查程序

CFCA 在开始一个可信任角色的雇佣关系前会依据以下流程对其进行审查：

（1）应聘者应提交的个人资料

履历、最高学历毕业证书、学位证书、资格证及身份证等相关的有效证明。

（2）应聘者个人身份的确认

CFCA 人力资源部门通过电话、信函、网络、走访、调阅档案等形式对其

提供材料的真实性进行鉴定。

（3）三个月的试用期考核

通过现场考试、日常观察、情景考验等方式对其考察。

以上三方面的审查结果必须符合第 5.3.1 节中规定的要求。

（4）签署保密协议

与到岗人员签署保密协议。

### 5.3.3 培训要求

CFCA 对录用人员按照其岗位和角色安排培训。培训内容有：PKI 的相关知识、岗位职责、内部规章制度、认证系统软件、相关应用软件、操作系统与网络、ISO9000 质量控制体系、ISO27001 信息安全管理体系、CP/CPS 等。

CFCA 处理证书业务相关的员工必须接受下列培训：

（1）向所有负责信息身份验证的职员（“验证专家”）提供技能培训。培训内容包括基础 PKI 知识、审核与验证制度和流程、对验证过程的主要威胁因素（如，网络钓鱼及其他社会工程学策略）以及证书标准；

（2）保留人员培训记录，并且确保“验证专家”能够胜任身份信息验证工作的技术要求；

（3）验证专家必须按其不同的技术水平等级被授予不同的签发证书权限，技术水平分级标准应与培训内容以及业绩考核标准一致；

（4）确保为验证专家分配签发证书权限前，不同技术水平等级的验证专家都具有足够的胜任能力；

（5）要求所有的验证专家通过关于证书标准中身份验证要求的 CA 内部考

试。

### 5.3.4再培训周期和要求

CFCA 每年至少向员工提供一次业务培训机会以不断提高其职业技能，以保持其完成工作所需要的职业水平。同时，当 CA 系统更新升级时也会对其员工进行相应的培训。

### 5.3.5工作岗位轮换周期和顺序

CFCA 根据具体工作情况安排并制定员工工作岗位的轮换周期与顺序。

### 5.3.6未授权行为的处罚

员工一旦被发现执行了未经授权的操作时，将被立即中止工作并受到纪律惩罚，其处理办法根据 CFCA 相关的管理规范执行。

### 5.3.7独立和约人的要求

CFCA 目前未聘用外部独立合约人从事认证相关的工作。

### 5.3.8提供给员工的文档

CFCA 向其员工提供完成其工作所必须的文档。

为了使认证系统的运营持续正常安全的运行，应该给相关员工提供有关的文档，至少包括：

（1）认证系统操作说明手册.

（2）CP/CPS 电子认证业务规则和有关的协议和规范。

（3）内部操作文件，包括备份手册、灾难恢复方案等。

（4）岗位说明。

（5）公司相关培训资料。

（6）相关安全管理规范。

## 5.4 审计日志程序

### 5.4.1 记录事件的类型

1、CA 证书及密钥生命周期管理事件：

（1）密钥的生成、备份、存储、恢复、归档和销毁。

（2）证书请求、续期和更新密钥请求，以及撤销。

（3）证书申请的批准和拒绝，包括成功或失败的证书操作。

（4）加密设备生命周期管理事件，包括：设备接收、安装、卸载、激活、使用、维修等。

（5） CRL 条目的生成。

（6）签署 OCSP 响应。

（7）引入新证书档案和淘汰现有证书档案的记录。

2、订户的生命周期管理事件：

（1）证书请求、更新、更新密钥请求和撤销。

（2）CA/Browser 论坛要求及本 CP/CPS 中规定的所有验证活动。

（3） 证书请求的接受和拒绝，包括接受订户协议，申请资料的验证、申请及验证资料的保存等。

（4）证书的签发。

（5）CRL 条目的生成。

（6）签署 OCSP 响应。

（7）多视角签发确证机制会从每个网络视角进行尝试，并至少记录以下信息：

- 用于唯一标识所使用网络视角的标识符；
- 尝试验证的域名和/或 IP 地址；
- 尝试结果（例如，“域名验证通过/失败”、“CAA 权限允许/禁止”）。

3. 安全事件：

（1）成功和不成功的 PKI 系统访问尝试。

（2）执行的 PKI 和安全系统行动。

（3）安全配置文件的更改。

（4）证书系统上软件的安装、更新和删除。

（5）系统崩溃、硬件故障和其他异常情况。

（6）防火墙和路由器活动。

（7）进入和离开 CA 设施的情况，包括授权人员与非授权人员及安全存储设施的进出访问。

4. 系统操作事件:

（1）系统启动和关闭。

（2）系统权限的创建、删除，设置或修改密码。

（3）对于 CA 系统网络的非授权访问及访问企图。

（4）对于系统文件的非授权的访问及访问企图。

（5）安全、敏感文件或记录的读、写或删除。

5. 可信人员管理记录：

（1）网络权限的帐号申请记录。

（2） 系统权限的申请、变更、创建申请记录。

（3） 人员情况变化。

上述日志信息包括记录时间、序列号、记录的实体身份、日志种类等。

### 5.4.2处理日志的周期

CFCA 对上条中 1 类日志由密钥管理员收集并管理；2、3 类日志由数据库保存，并每天进行一次增量备份，每周进行一次全备份；4 类日志每天自动保存在备份设备上；5 类日志每季度进行一次审计。

### 5.4.3审计日志的保存期限

CFCA 及其时间戳机构保留以下日志至少两年。

1、在以下情况发生后的 CA 证书和密钥生命周期管理事件记录（如第 5.4.1（1）规定）。

（1）CA 私钥销毁。

（2）证书中 X.509v3 基本约束扩展项的 CA 字段设定为“是”，且与该 CA 私钥享有共同公钥的最终 CA 证书被撤销或到期。

2、在订户证书撤销或过期后的订户证书生命周期管理事件记录（如第 5.4.1（2）节所述）。

3、当有事件发生后的任何安全事件记录（如第 5.4.1（3）条规定）。

注意：虽然这些要求设定了最短的保留期限，但 CFCA 可选择更大的时间期限值，以利于调查需要回溯和检查的可能发生的安全事件或其他类型的事件。

### 5.4.4 审计日志的保护

CFCA 建立了相应的管理制度，并采取物理和逻辑的控制方法确保只有经 CFCA 授权的人员才能对审计日志进行操作。审计日志处于严格的保护状态，严禁未经授权的任何操作。

### 5.4.5 审计日志备份程序

对于系统日志、数据库日志和相关业务日志，CFCA 将按照其《日志管理办法》及《数据备份管理办法》执行备份操作。

### 5.4.6 审计收集系统

应用程序、网络和操作系统等都会自动生成审计数据和记录信息。

关于电子审计信息，CFCA 的审计日志收集系统涉及：

1、 证书管理系统。

2、 证书签发系统。

3、 证书目录系统。

4、 证书受理系统。

5、 访问控制系统。

6、 网站、数据库安全管理系统。

7、 其他需要审计的系统。

8、 备份恢复系统

9、 用户服务系统

对于纸质审计信息，则有专门的文件柜来实现收集归档。

### 5.4.7对导致事件主体的通告

当 CFCA 发现被攻击时，将记录攻击者的行为，在法律许可的范围内追溯攻击者，保留采取相应对策措施的权利。CFCA 有权决定是否对事件相关实体进行通知。

### 5.4.8脆弱性评估

CFCA 每年至少会进行一次系统安全性评估：

1、识别可预见的可能导致未经授权访问、披露、滥用、更改或破坏任何证书数据或证书管理流程的内部和外部威胁。

2、评估这些威胁的可能性和潜在损害，同时考虑到证书数据和证书管理流程的敏感性。

3、评估 CA 为应对此类威胁而制定的政策、程序、信息系统、技术和其他安排的充分性。

## 5.5记录归档

### 5.5.1归档记录的类型

CFCA 归档的内容包括：

1、与证书系统、证书管理系统、根 CA 系统和委托第三方系统的安全性相关的文档。

2、 与证书请求和证书的验证、颁发和撤销相关的文档。

### 5.5.2归档记录的保存期限

存档的审计日志（如第 5.5.1 章中所述）将从其记录创建时间戳起至少保留 2 年，或者根据第 5.4.3 章要求保留的时间，两者以时间更长的为准。

CFCA 至少保留 2 年的记录包括：

1、第 5.5.1 章中规定的与证书系统、证书管理系统和根 CA 系统的安全相关的所有存档文件。

2、在发生以下情况后，与证书申请和证书（如第 5.5.1 章中规定）的验证、签发和撤销相关的所有存档文件。

（1）此类记录和文件最后依赖于证书请求和证书的验证、签发或撤销。

（2）依赖于此类记录和文件的订户证书的到期。

如果法律需要，CFCA 将调整记录保存期限。CRL 或 OCSP 中的证书吊销记录在此证书的有效期内不会被删除。

### 5.5.3归档文件的保护

CFCA 对归档文件有相应的保存制度。

对于电子形式的归档记录文件，确保只有被授权的可信任人员才允许访问存档数据，并通过适当的物理和逻辑访问控制防止对电子归档记录进行未授权的访问、修改、删除或其它操作。CFCA 将使用可靠的归档数据存储介质和归档数据处理应用软件，确保归档数据在其归档期限内只有被授权的可信任人员才能成功访问。

对于书面形式的归档记录文件，CFCA 制定了相应的档案管理办法，并设有专门的档案管理人员对书面档案进行妥善保存，并有相应的查阅制度确保只有经批准的人员方可访问书面归档记录。

### 5.5.4 归档文件的备份程序

归档文件的备份内容包括：数据库的备份、操作系统的备份及日志的备份。

数据库备份：采用本地备份和异地备份、增量备份与全部备份相结合的方式进行备份。

操作系统的备份：系统初次上线后进行一次备份，在系统有调整时进行备份。

### 5.5.5 记录的时间戳要求

归档的记录都需要标注时间；系统产生的记录按照要求添加时间标识。

### 5.5.6 归档收集系统（内部或外部）

CFCA 有自动的电子归档信息的存放系统。

### 5.5.7 获得和检验归档信息的程序

只有被授权的可信人员才能获得归档信息。当归档信息被恢复后会对其完整性进行检验。

## 5.6 电子认证服务机构密钥更替

当 CA 密钥对的累计寿命超过第 6.3.2 中规定的最大有效期时，CFCA 将启

动密钥更新流程，替换已经过期的 CA 密钥对。CFCA 密钥变更按如下方式进行：

一个上级 CA 应在其私钥到期时间小于下级 CA 的有效期之前停止签发新的下级 CA 证书（“停止签发日期”）。

产生新的密钥对，签发新的上级 CA 证书。

在“停止签发证书的日期”之后，对于批准的下级 CA（或最终订户）的证书请求，将采用新的 CA 密钥签发证书。

上级 CA 将继续利用原来的 CA 私钥签发 CRL 直到利用原私钥签发的最后的证书过期为止。

## 5.7 损坏与灾难恢复

### 5.7.1 事故和损害处理流程

当 CFCA 遭到攻击、发生通讯网络故障、计算机设备不能正常提供服务、软件遭破坏、数据库被篡改等情况时，CFCA 将根据其制订的业务持续计划等相关规章制度采取合理措施。

业务持续计划由“CFCA 运营安全管理委员会”（以下简称安委会）总负责，其职能包括指导和管理信息安全工作，批准、发布业务持续计划，根据实际情况决定启动灾难恢复等各项职能。安委会的成员包括公司领导与各部门负责人。

业务中断事件分紧急事件和灾难事件。当服务中断发生后，该中断对客户服务产生重大影响，但恢复服务不受外界因素的影响，短时间内即可恢复服务，这类事件称为紧急事件；当服务中断因不可抗力因素造成，比如自然灾害、传

染病、政治暴动等因素引起的事件称为灾难事件。

CFCA 针对不同事件制定了相应的应急处理机制。

当发生紧急事件后，安委会负责人召集安委会成员举行会议，对事件进行评估。运行部按照确定的处理机制进行处理，市场部、技术部根据实际情况，针对受影响客户进行妥善处理。在紧急事件应急处置后，CFCA 将评估已有风险防范措施的有效性并加以改进。

当发生灾难事件时，按照 5.7.4 的规定进行。

对于一般故障，CFCA 将在 2 小时内解决；对于紧急事件，CFCA 在 24 小时内解决；对于灾难性事件，在主运营场地出现灾难事故或不可抗力事故而不能正常运营时，CFCA 将在 48 小时内，利用备份数据和设备在数据备份中心恢复电子认证服务。

对于全球信任体系下的证书，CFCA 还具有专门的问题报告和响应能力：

（1）CFCA 向订户、依赖方、软件开发商和其他的第三方提供了 7*24 服务热线（400-880-9888），说明如何向 CFCA 报告证书的投诉、私钥泄漏、证书使用不当、或其他形式的欺诈、泄漏、使用不当或行为不当。

（2）CFCA 将在问题报告的 24 小时内开始进行调查，并至少根据以下的条件来判断是否采取吊销或其它相应手段：

问题的性质；

收到的对特定证书或网站问题报告数量；

投诉人的身份；

相关的法规。

（3） CFCA 可确保全天候（7*24 小时）对高优先级的问题报告首先在 CA

内部进行响应。然后，在有必要时将这些问题提交给法律机构或执行证书的吊销。

### 5.7.2 计算资源、软件和/或数据的损坏

当计算资源、软件和/或数据受到破坏后，将依据 5.7.1 中的规定区分是紧急事件还是灾难事件，按照不同的事件分类根据相应的处理流程进行处理。

### 5.7.3 实体私钥损害处理程序

CFCA 制定了根私钥泄露的应急预案，其中明确规定了根私钥泄露的内部处理流程、人员分工及对外通知处理流程。

当 CFCA 证实根私钥发生泄露时，将会立即上报行业主管部门，说明发生根私钥泄露的时间、原因以及采取的应急处理措施。

CFCA 一旦证实根私钥泄露时，会立即通过官网等方式通知订户及依赖方，对所有证书进行吊销，并不再签发新的证书。

1、当证书订户发现证书私钥损害时，订户必须立即停止使用其私钥，并立即访问 CFCA 证书服务站点撤销其证书，或立即通过电话邮件等方式通知 CFCA 撤销其证书，并按照相关流程重新申请新的证书。CFCA 将按本 CP/CPS 第 4.9 节发布证书撤销信息。

2、当 CFCA 证书订户的证书私钥受到损害时，CFCA 将立即撤销证书，通知证书订户；订户必须立即停止使用其私钥，并按照相关流程重新申请新的证书。CFCA 将按本 CP/CPS 第 4.9 节发布证书撤销信息。

3、当 CFCA 的根 CA 或中级 CA 出现私钥损害时，CFCA 将按照密钥应

急方案进行紧急处理，并及时通过各种途径通知依赖方，如：Microsoft、Mozilla、Google、Apple、Adobe、Oracle、360。

### 5.7.4 灾难后的业务连续性能力

CFCA 建有数据备份中心，有相应的业务持续计划，可确保灾难后的业务连续性能力。

在主运营场地出现灾难事故或不可抗力事故而不能正常运营时，CFCA 将在 48 小时内，利用备份数据和设备在数据备份中心恢复电子认证服务。

## 5.8 电子认证服务机构或注册机构的终止

CFCA 拟终止电子认证服务时，将在终止服务六十日前向行业主管部门报告，并办理电子认证服务资质的注销手续。

CFCA 拟暂停或者终止电子认证服务的，将在暂停或者终止电子认证服务九十日前，就业务承接及其他有关事项通知注册机构、订户、依赖方等有关各方，并依据与注册机构签署的合作协议向注册机构进行赔偿，依据对订户和依赖方的数字证书服务协议向订户和依赖方进行赔偿；向电子认证业务承接方提供认证相关信息，包括但不限于：证书办理资料、证书信息库、最新的证书状态资料等。

CFCA 将在暂停或者终止电子认证服务六十日前向行业主管部门报告，并与其他电子认证服务机构就业务承接进行协商，作出妥善安排。

若 CFCA 未能就业务承接事项与其他电子认证服务机构达成协议的，将申请行业主管部门安排其他电子认证服务机构承接相关业务。

行业主管部门对此有其他相关要求的，CFCA 将严格按照行业主管部门的要求进行。

# 6 认证系统技术安全控制

## 6.1 密钥对的生成和安装

### 6.1.1 密钥对的生成

1、 CA密钥对的生成

CA 的密钥对在加密机内部产生，加密机具有国家密码主管部门的相应资质。加密机采用密钥分割或秘密共享机制进行备份。在生成 CA 密钥对时，CFCA 按照加密机密钥管理办法，执行详细的操作流程控制计划，选定并授权 5 个密钥管理员，密钥管理员凭借口令和智能 IC 卡对密钥进行控制。在第三方审计人员的监督下，由 5 名中的 3 名具有密钥管理及操作权限的人员同时到达 CFCA 最安全区同时进行操作，产生 CA 密钥，并由第三方审计人员出具报告表明 CFCA 在 CA 密钥对生成过程中的流程和控制能够保证 CA 密钥对的完整性和机密性。CA 密钥的生成、保存和密码模块符合国家密码主管部门的要求，并具有国家密码主管部门的相应资质。

2、RA密钥的生成

RA 的签名私钥在安全控制下产生，RA 证书由 CFCA 签发。

3、订户密钥的生成

CFCA 不替订户生成密钥对，由订户自行生成，订户应确保其密钥对产生的可靠性，并负有保护其私钥安全的责任和义务，并承担由此带来的法律责任。

CFCA 拒绝符合以下情况的订户证书申请。

（1）密钥对不满足本 CP/CPS 6.1.5 或 6.1.6 中的要求。

（2）有明确的证据表明，订户用于生成私钥的具体方法是有缺陷的。

（3）已泄露的订户私钥，如 CFCA 通过已验证的方法可推演出订户私钥。

（4）CFCA 已事先获知订户的私钥已遭泄露(例如通过本 CP/CPS 4.9.1.1 中规定的情形获知)。

（5）对于业界证明的弱私钥。CFCA 对于 2024 年 11 月 15 日或之后提交的请求，采取以下预防措施：

①在 Debian 弱密钥漏洞(https://wiki.debian.org/SSLkeys)的情况下，CFCA 拒绝在 https://github.com/cabforum/Debian-weak-keys/中找到的所有密钥，针对存储库中列出的每种密钥类型（例如 RSA、ECDSA）和大小。对于满足本 CP/CPS 6.1.5 中要求的所有其他密钥，除 RSA 密钥大小大于 8192 位外，CFCA 拒绝 Debian 弱密钥。

②在存在 ROCA 漏洞的情况下，CFCA 拒绝通过 https://github.com/crocs-muni/roca 或同等工具识别的密钥。

③在 Close Primes 漏洞(https://fermatattack.secvuln.info/)的情况下，CFCA 拒绝可使用费马分解方法在 100 轮内分解的弱密钥。

### 6.1.2 私钥传送给订户

订户的私钥是由订户自己生成，不会进行传送。

### 6.1.3公钥传送给证书签发机构

在申请服务器证书时，订户在其服务器设备上生成密钥对后，应当将包含公钥信息的证书签名请求文件（CSR）通过适当的的形式（如电子邮件、在线平台提交等）发送给 CFCA。

### 6.1.4电子认证服务机构公钥传送给依赖方

用于验证 CFCA 签名的验证公钥，包含 CFCA 的根 CA 证书和中级 CA 证书，可从 CFCA 的官网获得。

### 6.1.5密钥的长度

CFCA 遵从国家法律法规、政府主管机构等对密钥长度的明确规定和要求，目前：

CFCA 全球信任体系下的 CA 签名密钥长度及算法如下：

CFCA EV ROOT—RSA-4096/SHA-256

CFCA EV OCA—RSA-2048/SHA-256

CFCA OV OCA—RSA-2048/SHA-256

CFCA DV OCA—RSA-2048/SHA-256

CFCA Global ECC ROOT G2—ECC-384（NIST P-384）/SHA-384

CFCA EV ECC OCA G2—ECC-384（NIST P-384）/SHA-384

CFCA OV ECC OCA G2—ECC-384（NIST P-384）/SHA-384

CFCA DV ECC OCA G2—ECC-384（NIST P-384）/SHA-384

CFCA Global RSA ROOT G2—RSA-4096/SHA-512

CFCA EV RSA OCA G2—RSA-4096/SHA-256

CFCA OV RSA OCA G2—RSA-4096/SHA-256

CFCA DV RSA OCA G2—RSA-4096/SHA-256

订户密钥的长度为 RSA-2048、RSA-4096 或者 ECC-256（NIST P-256）。

### 6.1.6 公钥参数的生成和质量检查

CFCA 和订户均需遵循本 CP/CPS 6.1.1 中的规定生成公钥，公钥参数由合规的设备/平台生成以保证公钥参数的质量，公钥需满足本 CP/CPS 6.1.5 中的要求。

CFCA 在签发证书前，进行公钥参数检测，以确保公钥参数满足以下:

对于 RSA 公钥:

1、 公共指数为大于或等于 3 的奇数。

2、 公共指数范围应在 2^16+1~2^256-1 之间。

3、 模数为奇数。

4、 模数位数至少 2048 位且是 8 的整数倍。

5、 模数不是质数的幂。

6、 模数没有小于 752 的因数。

对于 ECDSA 公钥：

所有密钥的有效性都通过完整的 ECC 公钥验证程序或 ECC 部分公钥验证程序来确认。

### 6.1.7 密钥使用目的（依据 X.509 v3 密钥用途字段）

CFCA 签发的 X.509 v3 证书包含了密钥用法扩展项，其用法与 RFC 5280 标准相符。对于 CFCA 在其签发证书的密钥用法扩展项内指明了的用途证书订户必须按照该指明的用途使用密钥。

根 CA 密钥一般用于签发以下证书和 CRL：

1、代表根 CA 的自签名证书。

2.、中级 CA 的证书、交叉证书。

3.、OCSP 响应签名证书。

中级 CA 密钥一般用于签发以下证书和 CRL：

1、订户证书。

2、时间戳签名证书。

3、OCSP 响应签名证书。

## 6.2 私钥保护和密码模块工程控制

### 6.2.1 密码模块标准和控制

CFCA 实施物理和逻辑保护措施以防止未经授权的证书签发。在上述指定的已验证系统或设备之外的私钥备份，CFCA 将密钥片段加密存储在不同实体的物理设备中，以防止私钥泄漏。加密私钥片段所使用的算法以及密钥长度根据现有技术，该算法和密钥长度能够在加密密钥或密钥部分的剩余生命周期内抵御密码分析攻击。

CFCA 用于 CA 密钥对的加密模块均符合 FIPS 140-2 级别 3 标准。

### 6.2.2私钥多人控制

CFCA CA 密钥存放在加密机中，加密机的管理密钥被分割保存在 3 张 IC 卡中，IC 可分别由 3 位经过授权的安全管理员掌握，并保存在屏蔽机房中的最安全区内的保险箱中。

CA 私钥的生成、更新、撤销、备份和恢复等操作采用多人控制机制将私钥的管理权限分散到 5 位密钥管理员中，至少在 3 人及以上的密钥管理员在场并许可的情况下，插入管理员 IC 卡并输人 PIN 码，才能对私钥进行操作。

### 6.2.3私钥托管

对于 CA 私钥，CFCA 无托管业务。

### 6.2.4私钥备份

CA 的私钥由加密机产生，加密机有双机备份，并保存在防高温、防潮湿及防磁场影响的环境中，对加密机的备份操作须 3 人以上(包括 3 人)才可完成。

订户的私钥由订户产生，建议订户自行备份，并对备份的私钥采用口令或其他访问控制机制保护，防止非授权的修改或泄漏。

### 6.2.5私钥归档

当 CFCA 的 CA 密钥对到期后，这些密钥对将被归档保存至少 10 年。归档的 CA 密钥对保存在本 CP/CPS 6.2.1 章节所述的硬件密码模块中，并且 CFCA 的密钥管理策略和流程都确保了归档后的 CA 密钥对不会再被用于生产系统中。当归档 CA 密钥对达到归档保存期限之后，CFCA 将按照本 CP/CPS6.2.10 所述

的方法进行安全地销毁。

### 6.2.6私钥导入、导出密码模块

CFCA 通过硬件模块生成 CA 密钥对，部署了备份加密设备，CA 密钥对在备份传递时以离线加密方式进行,并且在传递前要进行身份鉴别，以防止 CA 私钥的丢失、被窃、修改、非授权的泄露、非授权的使用。

通过硬件产生的订户私钥不能导出密码模块。其他方法产生的订户私钥在导出时应采取加密的方式进行。

### 6.2.7私钥在密码模块的存储

CFCA 私钥以加密的形式存放在符合 FIPS 140-2 级别 3 标准的硬件密码模块中。

### 6.2.8激活私钥的方法

CFCA 采用硬件设备（加密机）产生、保存 CA 私钥，其激活数据按照本 CP/CPS6.2.2 要求进行分割。须由 3 个管理员共同操作才能完成激活，一旦 CA 私钥被激活，激活状态将保持到 CA 离线。

### 6.2.9解除私钥激活状态的方法

对于 CA 私钥，当硬件密码模块断电、重新初始化、移开令牌/钥匙，私钥进入非激活状态，未经授权的任何人员，不可以进行相关操作。

### 6.2.10 销毁私钥的方法

当 CA 的生命周期结束后，CFCA 将根据本 CP/CPS 6.2.5 之相关规定将 CA 私钥进行归档，其它的 CA 私钥备份将被安全销毁。归档的私钥在其归档期结束后，需要在 3 名以上可信人员参与下进行安全地销毁。

### 6.2.11 密码模块的评估

CFCA 用于 CA 密钥对的加密模块均符合 FIPS 140-2 级别 3 标准。

## 6.3 密钥对管理的其它方面

### 6.3.1 公钥归档

公钥归档的保存期限、保存机制、安全措施等与证书保持一致。归档要求参照本 CP/CPS 5.5 的相关规定。

### 6.3.2 证书操作期和密钥对使用期限

CA 证书的有效期不超过 25 年，EV/OV/DV SSL 证书有效期遵循基本要求，具体如下：

订户证书最长有效期参考表

| 证书签发日期在此及之后 | 证书签发日期在此之前 | 最大有效期 |
|---|---|---|
| | 2026 年 3 月 15 日 | 397 天 |
| 2026 年 3 月 15 日 | 2027 年 3 月 15 日 | 199 天 |
| 2027 年 3 月 15 日 | 2029 年 3 月 15 日 | 99 天 |

| | | |
|---|---|---|
| 2029 年 3 月 15 日 | | 46 天 |

CA 密钥对使用期限不超过 25 年。订户证书的密钥对使用期限不做规定。

## 6.4 激活数据

### 6.4.1 激活数据的产生和安装

1、CFCA 的 CA 私钥的激活数据产生遵循本 CP/CPS6.2.2 中的要求；

2、对于订户，激活数据是保护私钥的密码。CFCA 推荐订户使用强口令来保证私钥的安全性，该口令需要：

- 至少为 8 位字符。
- 至少包含一个字符和一个数字。
- 至少包含一个小写字母。
- 建议订户不要使用生日、简单重复的数字等容易被人猜中或破解的信息做为口令。
- 建议定期修改。

### 6.4.2 激活数据的保护

1、CFCA 的密钥管理者须保护他们所维护的秘密份额，并且须签署协议来承诺所承担的责任。

2、对于 CA 私钥的激活数据，CFCA 将激活数据按照可靠的方式分割后由不同的密钥管理人员掌管。

3、订户必须以加密的形式保存私钥，建议使用双因素认证（如硬件设备加强口令）来保护其私钥。

4、订户的激活数据必须进行妥善保管，防止泄露和窃取。

### 6.4.3激活数据的其他方面

#### 6.4.3.1 激活数据的传输

存有CA私钥的加密设备和相关IC卡，通常被保存在CFCA最安全区机房，不能携带离开CFCA。如在某种特殊情况下需要进行传输时（如建设灾备系统时），其传送过程需要在CFCA安全管理人员和密钥管理人员共同监督的情况下进行。

对于证书订户，通过网络传输用于激活私钥的口令时，需要采取加密等保护措施，以防丢失。

#### 6.4.3.2 激活数据的销毁

CFCA通过对设备初始化的方式来销毁CA私钥的激活数据。

订户私钥的激活数据在不需要时由订户自行销毁，订户应确保他人无法通过残余信息、存储介质直接或间接地恢复激活数据。

## 6.5计算机安全控制

根据系统安全管理的相关规定，CFCA要求CA与RA系统采用可信安全操作系统对外提供服务。企业客户也必须使用可信任操作系统。

### 6.5.1特别的计算机安全技术要求

CFCA的信息安全管理符合国家相关规定，主要安全技术和控制措施包括：

采用安全可信任的操作系统、严格的身份识别和人员访问控制制度、多层防火墙设置、人员职责分割、内部操作控制、业务持续计划等各方面。

CFCA 对于可直接导出证书签发的账户实施多因子身份认证。

### 6.5.2 计算机安全评估

CFCA 全球信任证书认证系统已通过国家密码管理局等有关部门的安全性审查。

## 6.6 生命周期技术控制

### 6.6.1 系统开发控制

CFCA 的开发控制包括可信人员管理、开发环境安全管理、产品设计和开发评估、使用可靠的开发工具等，设计的生产系统满足冗余性、容错性、模块化的要求。软件设计和开发过程遵循以下原则：

制定公司内部的升级变更申请制度，并要求工作人员严格按照流程执行:

1、制定公司内部的采购流程及管理制度。

2、开发程序必须在开发环境进行严格测试成功后，再申请部署于生产环境。

3、变更部署前进行有效的在线备份。

4、第三方验证和审查。

5、安全风险分析和可靠性设计。

同时 CFCA 的系统由符合国家相关安全标准和具有商用密码产品生产资质的可靠开发商开发，其开发过程符合国家密码主管部门的相关要求。

### 6.6.2安全管理控制

CFCA 认证服务系统的信息安全管理，严格遵循行业主管部门的规范进行操作，系统的任何变更都经过严格的测试验证后才能进行安装和使用。同时，按照 ISO9000 质量管理体系、ISO27001 信息安全管理体系标准建立了严格的管理制度。对于核心数据，安排专人定时进行备份，每月由专人负责数据恢复，以验证数据的有效性。

### 6.6.3生命期的安全控制

CFCA 的系统由符合国家相关安全标准和具有商用密码产品生产资质的可靠开发商开发，其开发过程符合国家密码主管部门的相关要求，其产品源代码在国家密码主管部门处留有备份，以保证系统的延续性。

## 6.7网络安全控制

CFCA 认证系统通过以下手段来防止网络受到未授权的访问和抵御恶意攻击：

1、由路由器对来自外部的访问信息进行过滤控制。

2、将功能独立的服务器放置在不同的网段。

3、多级防火墙划分不同网段，并采用了完善的访问控制技术。

4、通过验证和存取访问权限控制进行数据保护。

5、在网络系统中，采用入侵检测产品，从检测与监听等多方面对网络系统进行防护，及时发现入侵者并报警，并实施事件响应。

6、所有终端安装防病毒软件，并定期升级。

7、提供冗余设计。

## 6.8时间信息

证书、CRL、OCSP、电子认证服务系统日志均包含时间信息，该时间信息来源于国家的标准时间源。

# 7 证书、证书吊销列表和在线证书状态协议

## 7.1证书

### 7.1.1版本号

CFCA 签发的证书格式符合 X.509 V3 标准，这一版本信息包含在证书版本属性内。

### 7.1.2证书扩展项

CFCA 在按照 RFC5280 规定要求基础上，以下配置盖所有签发的证书。

7.1.2.1 根证书配置

7.1.2.3 技术受限的非 TLS 中级证书配置

7.1.2.6 TLS 中级 CA 证书配置

7.1.2.7 订户证书配置

7.1.2.8 OCSP 响应程序证书配置

7.1.2.9 预证书配置

#### 7.1.2.1 根 CA 证书配置

见第 11.1 节。

##### 7.1.2.1.1 根 CA 有效性

见第 11.1 节。

##### 7.1.2.1.2 根 CA 扩展

见第 11.1 节。

##### 7.1.2.1.3 根 CA 机构密钥标识符

见第 11.1 节。

##### 7.1.2.1.4 根 CA 基本约束

见第 11.1 节。

#### 7.1.2.2 交叉认证的中级 CA 证书配置

不适用。

##### 7.1.2.2.1 交叉认证的中级 CA

不适用。

#### 7.1.2.2.2 交叉认证的中级 CA 命名

不适用。

#### 7.1.2.2.3 交叉认证的中级 CA 扩展

不适用。

#### 7.1.2.2.4 交叉认证的中级 CA 扩展密钥用法-无约束

不适用。

#### 7.1.2.2.5 交叉认证的中级 CA 扩展密钥用法-受约束

不适用。

#### 7.1.2.2.6 交叉认证的中级 CA 证书策略

不适用。

### 7.1.2.3 技术受限的非 TIS 中级 CA 证书配置

CFCA 除了 TLS 证书以外，还会 AATL 证书、OCSP 应用程序响应证书。配置可见附件 11 章节。

#### 7.1.2.3.1 技术受限的非 IIS 中级 CA 扩展

见第 11 章节。

#### 7.1.2.3.2 技术受限的非 TLS 中级 CA 证书策略

见第 11 章节。

#### 7.1.2.3.3 技术受限的非 TLS 中级 CA 扩展密钥用法

见第 11 章节。

### 7.1.2.4 技术受限的预证书签名 CA 证书配置

不适用。

#### 7.1.2.4.1 技术受限的预证书签名 CA 扩展

不适用。

#### 7.1.2.4.2 技术受限的预证书签名 CA 扩展密钥用法

不适用。

### 7.1.2.5 技术受限的 TLS 中级 CA 证书配置

不适用。

#### 7.1.2.5.1 技术受限的中级 CA 扩展

不适用。

#### 7.1.2.5.2 技术受限的中级 CA 名称约束

不适用。

### 7.1.2.6 中级 CA 证书配置

见第 11.2 节。

#### 7.1.2.6.1 中级 CA 扩展

见第 11.2 节。

### 7.1.2.7 订户（服务器）证书配置

CFCA 签发 TLS 证书可以见附件 11.3，另外也签发文档签名证书用的订户证书，以及 OCSP 应用程序响应证书，可以见附件 11.3。

#### 7.1.2.7.1 订户证书类型

TLS 证书包括：域名验证型(DV)，组织验证型(OV)，增强验证型(EV)。

其它包括：文档签名证书(DS)、以及 OCSP 应用程序响应证书。

#### 7.1.2.7.2 域名验证

见第 11.3 节。

#### 7.1.2.7.3 个人验证

不适用。

#### 7.1.2.7.4 组织验证

见第 11.3 节。

#### 7.1.2.7.5 增强验证

见第 11.3 节。

#### 7.1.2.7.6 订户证书扩展

见第 11.3 节。

#### 7.1.2.7.7 订户证书签发机构信息访问

见第 11.3 节。

#### 7.1.2.7.8 订户证书基本约束

见第 11.3 节。

#### 7.1.2.7.9 订户证书策略

见第 11.3 节。

#### 7.1.2.7.10 订户证书扩展密钥用法

见第 11.3 节。

#### 7.1.2.7.11 订户证书密钥用法

见第 11.3 节。

#### 7.1.2.7.12 订户证书主题备用名称

见第 11.3 节。

### 7.1.2.8 OCSP 应用程序响应证书配置

见第 11.4 节。

#### 7.1.2.8.1 OCSP 应用程序响应证书有效期

见第 11.4 节。

#### 7.1.2.8.2 OCSP 应用程序响应证书扩展

见第 11.4 节。

#### 7.1.2.8.3 OCSP 应用程序响应证书权限信息访问

不适用。

#### 7.1.2.8.4 OCSP 应用程序响应证书基本约束

见第 11.4 节。

#### 7.1.2.8.5 OCSP 应用程序响应证书扩展密钥用法

见第 11.4 节。

#### 7.1.2.8.6 OCSP 应用程序响应证书 id-pkix-ocsp-nocheck

见第 11.4 节。

#### 7.1.2.8.7 OCSP 应用程序响应证书密钥用法

见第 11.4 节。

#### 7.1.2.8.8 OCSP 应用程序响应证书策略

不适用。

### 7.1.2.9 预证书配置

预证书是一个由 RFC 6962 定义的数据结构，可以提交到证书透明度日志中。在结构上 Precertificate 与证书完全相同，唯一区别是在扩展字段中具有特殊的关键性扩展 Precertificate Poison(OID: 1.3.6.1.4.1.11129.2.4.3)。该扩展确保预证书不会被符合 RFC 5280 的客户端接受为证书。签署的预证书的存在可以被视为相应证书也存在的证据，因为签名代表 CFCA 的承诺，他可以签发这样的证书。

预证书在 CA 决定签发证书之后，但在实际签署证书之前创建。CFCA 可以构建和签发与证书对应的预证书，用于提交到证书透明度日志。CFCA 可以使用返回的签名证书时间戳来修改证书的扩展字段，在签署证书之前添加一个签名证书时间戳列表，如第 7.1.2.11.3 节中定义的，并根据相关配置文件允许的内容进行。

一旦签署了预证书，依赖方可以将其视为 CFCA 意图签发相应证书的有约束力承诺，或更常见的是，相应证书已经存在。证书是否与预证书相对应是根据待签名证书内容的值来确定的，该值经过 RFC 6962 第 3.2 节定义的转换过程。CFCA 在愿意签发相应证书时，才会签发预证书。预证书由签名 CA 直接签发。预证书配置中的字段中的编码与证书内容逐字逐句匹配，字段与 11.3 中 TLS 证书配置中的字段一致，序列号与相应证书字段相同。扩展部分见 7.1.2.9.1。

#### 7.1.2.9.1 预证书扩展配置-直接签发

| 扩展 | 是否存在 | 关键 | 描述 |
|---|---|---|---|
| Precertificate Poison (OID:1.3.6.1.4.1.11129.2.4.3) | 是 | 是 | |
| 签名证书时间戳列表 | 不 | - | |
| 其它扩展 | - | - | 与证书一致 |

#### 7.1.2.9.2 预证书扩展配置-预签名 CA 签发

不适用。

#### 7.1.2.9.3 预证书扩展

预证书包含预证书扩展（OID：1.3.6.1.4.1.11129.2.4.3）。

此扩展有一个 extnValue OCTET STRING，它正好是 RFC 6962 第 3.1 节规

定的 ASN.1 NULL 值的编码表示，即十六进制编码字节 0500。

#### 7.1.2.9.4 预证书授权密钥标识符

预证书由签名 CA 直接签发，预证书的授权密钥标识与签名 CA 的证书的主题密钥标识符一致。

### 7.1.2.10 CA 通用字段

CFCA 在签发 CA 证书之前，确保证书内容，包括每个字段的内容，完全符合第 7.1.2 节中至少一个证书配置文件的所有要求。

#### 7.1.2.10.1 证书有效期

见第 11.2 节。

#### 7.1.2.10.2 CA 证书命名

见第 11.2 节。

#### 7.1.2.10.3 CA 证书签发机构信息访问

见第 11.2 节。

#### 7.1.2.10.4 CA 证书基本约束

见第 11.2 节。

#### 7.1.2.10.5 CA 证书策略

见第 11.2 节。

#### 7.1.2.10.6 CA 证书扩展密钥用法

见第 11.2 节。

#### 7.1.2.10.7 CA 证书密钥用法

见第 11.2 节。

#### 7.1.2.10.8 CA 证书名称约束

不适用。

### 7.1.2.11 通用证书字段

CFCA 在签发证书之前，确保证书内容，包括每个字段的内容，完全符合第 7.1.2 节中至少一个证书配置文件的所有要求。

#### 7.1.2.11.1 授权密钥标识符

见第 11.3 节。

#### 7.1.2.11.2 CRL 分发点

见第 11.3 节。

#### 7.1.2.11.3 签名证书时间戳列表

如果存在签名时间戳列表扩展，其内容是一个 OCTET STRING，其中包含根据 RFC 6962 第 3.3 节规定编码的签名时间戳列表。

签名时间戳列表中包含的每个签名时间戳对应于与当前证书相关的预证书的 LogEntryType。

#### 7.1.2.11.4 主题密钥标识符

见第 11.3 节。

#### 7.1.2.11.5 其它扩展

见第 11.3 节。

### 7.1.3 算法对象标识符

#### 7.1.3.1 主题公钥信息

以下要求适用于证书或者预证书 subjectPublicKeyInfo，不使用其它编码。

##### 7.1.3.1.1 RSA

CFCA 使用 rsaEncryption（OID：1.2.840.113549.1.1.1）算法标识符指示 RSA 密钥，并且显示 NULL，编码时，RSA 的密钥算法标识符 16 进制编码为 300d06092a864886f70d0101010500。

#### 7.1.3.1.2 ECDSA

CFCA 使用 id-ecPublicKey（OID：1.2.840.10045.2.1）算法标识符指示 ECDSA 密钥。

参数使用曲线名称编码：

对于 P-256 密钥，曲线是 secp256r1（OID：1.2.840.10045.3.1.7）。

对于 P-384 密钥，曲线是是 secp384r1（OID：1.3.132.0.34）。

编码时，ECDSA 的密钥标识为以下 16 进制编码：

P-256 密钥 301306072a8648ce3d020106082a8648ce3d030107

P-384 密钥 301006072a8648ce3d020106052b81040022

### 7.1.3.2 签名算法标识符

CFCA 私钥来签名的对象以及派生出来的内容签名均符合上下文中所使用的算法。

特别是以下所有对象和字段：

1、证书或预证书的 signatureAlgorithm 字段。

2、待签名证书的 signature 字段。

3、证书列表的 signatureAlgorithm 字段。

4、待签名证书的 signature 的字段。

5、OCSP 响应的 signatureAlgorithm 字段。

#### 7.1.3.2.1 RSA

CFCA 使用 RSA 签名算法和编码，如下：

| 签名算法 | OID | 16 进制编码 |
| --- | --- | --- |
| SHA-256 with RSA | 1.2.840.113549.1.1.11 | 300d06092a864886f70d01010b0500 |
| SHA-384 with RSA | 1.2.840.113549.1.1.12 | 300d06092a864886f70d01010c0500 |
| SHA-512 with RSA | 1.2.840.113549.1.1.13 | 300d06092a864886f70d01010d0500 |

#### 7.1.3.2.2 ECDSA

CFCA 使用 ECDSA 签名算法和编码，如下：

| 签名算法 | OID | 16 进制编码 |
| --- | --- | --- |
| SHA-256 with ECDSA | 1.2.840.10045.4.3.2 | 300a06082a8648ce3d040302 |
| SHA-384 with ECDSA | 1.2.840.10045.4.3.3 | 300a06082a8648ce3d040303 |

### 7.1.4 名称形式

本节介绍了适用于 CA 签发的所有证书的编码规则。第 7.1.2 节中可能会规定进一步的限制，但这些限制不会取代这些要求。

#### 7.1.4.1 名称编码

CFCA 对于每个有效的认证路径（由 RFC 5280 第 6 节定义）：

（1）对于证书路径中的每个证书，证书的签发者甄别名字段的编码内容与签发 CA 证书的主题甄别名字段的编码形式逐字节相同。

（2）对于认证路径中的每个 CA 证书，证书的主题甄别名字段的编码内容在其主题可区分名称可以根据 RFC 5280 第 7.1 节进行比较的所有证书中逐字节相同，并且包括过期和撤销的证书。

在编码名称时：

（1）每个名称（Name）包含一个 RDNSequence。

（2）每个相对甄别名（RelativeDistinguishedName）恰好包含一个 AttributeTypeAndValue。

（3）如果存在多个相对甄别名，则它们按照它们在第 7.1.4.2 节中出现的顺序编码在 RDNSequence 内，可以参考附录 B。

（4）每个名称在所有相对甄别名中不包含多个给定的 AttributeTypeAndValue 实例。

### 7.1.4.2 主题属性编码

CFCA 签发的 TLS/CS 证书主体中属性顺序以及编码遵循如下表，其它证书参考附录 B 中对应的证书模版。通用名称包含一个 IP 地址或者 FQDN 的值，这个值存在于使用者备用名称扩展中。

| 属性 | OID | 规范 | 编码要求 | 最大长度 |
|---|---|---|---|---|
| 国家 | 2.5.4.6 | RFC5280 | PrintableString | 2 |
| 省份 | 2.5.4.8 | RFC5280 | UTF8String 或 PrintableString | 128 |
| 城市 | 2.5.4.7 | RFC5280 | UTF8String 或 PrintableString | 128 |
| 组织 | 2.5.4.10 | RFC5280 | UTF8String 或 PrintableString | 64 |
| 通用名称 | 2.5.4.3 | RFC5280 | UTF8String 或 PrintableString | 64 |

EV 相关属性顺序以及编码如下表。

| 属性 | OID | 规范 | 编码要求 | 最大长度 |
|---|---|---|---|---|
| businessCategory | 2.5.4.15 | X.520 | UTF8String 或 PrintableString | 2 |
| jurisdictionCountry | 1.3.6.1.4.1.311.60.2.1.3 | EVG | PrintableString | 128 |
| jurisdictionStateOrProvince | 1.3.6.1.4.1.311.60.2.1.2 | EVG | UTF8String 或 PrintableString | 128 |

| | | | | |
|---|---|---|---|---|
| jurisdictionLocality | 1.3.6.1.4.1.311.60.2.1.1 | EVG | UTF8String 或 PrintableString | 64 |
| serialNumber | 2.5.4.5 | RFC5280 | PrintableString | 64 |

#### 7.1.4.3 订户证书通用名称属性

通用名称包含的条目存在与使用者备用名称中，该字段值的编码如下：

（1）如果该值是 IPv4 地址，则该值必须编码为 IPv4 地址，如 RFC 3986 第 3.2.2 节中指定。

（2）如果该值是 IPv6 地址，则该值必须以 RFC 5952 第 4 节中指定的文本表示形式进行编码。

（3）如果 DNSName 值是完全限定域名或通配符域名，则该值编码与使用者备用名称中条目值逐字逐句匹配。完全限定域名或通配符域名的 FQDN 部分的所有域标签编码为 LDH-Label，并且 P-Label 不使用其 Unicode 表示形式。

#### 7.1.4.4 其他主题属性

见第 11.3 节。

### 7.1.5 名称限制

不适用。

### 7.1.6 证书策略对象标识符

#### 7.1.6.1 保留证书策略标识符

同本 CP/CPS 第 1.2 节。

### 7.1.7策略限制扩展项的用法

不适用。

### 7.1.8策略限定符的语法和语义

不适用。

### 7.1.9关键证书策略扩展项的处理规则

不适用。

## 7.2 证书撤销列表

2024-03-15 日起，CFCA 按照以下配置来生成并发布 CRL。

CRL 覆盖该 CA 所有的签发的证书。如果使用 CRL 分区，则这些分区的聚合等于完整的 CRL。CA 不间接签发 CRL。

| 属性 | | 是否存在 | 描述 |
|---|---|---|---|
| tbsCertList | | | |
| | version | 存在 | v2 版本 |
| | signature | 存在 | |
| | issuer | 存在 | 与签发 CA 主题逐字逐句匹配 |
| | thisUpdate | 存在 | CRL 的签发日期 |
| | nextUpdate | 存在 | 订户证书 7 天，中级证书 12 个月 |
| | revokedCertificate | 不使用 | |
| | extensions | 存在 | 见下表 |
| signature | | 存在 | |

### 7.2.1版本号

CFCA 的证书撤销列表符合 X.509 v2 的版本及格式要求。

## 7.2.2CRL 和 CRL 条目扩展项

CRL 扩展：

| 扩展 | 是否存在 | 是否关键 | 描述 |
|---|---|---|---|
| authorityKeyIdentifier | 是 | 非 | 与签发 CA 的 SubjectKeyIdentifier 逐字逐句匹配 |
| CRLNumber | 是 | 非 | 为非负且不超过 2^159 次方的递增的整数 |
| IssuingDistributionPoint | * | - | 见本 CP/CPS 7.2.2. |

撤销证书组件：

| 组件 | 是否存在 | 描述 |
|---|---|---|
| serialNumber | 是 | 与撤销证书的序列号逐字逐句匹配 |
| revocationDate | 是 | 通常为撤销日期，如果 CFCA 有充足的证据表明该证书私钥泄漏日期早于撤销日期，那么此日期将回溯到该泄漏日期。 |
| crlEntryExtensions | 可能 | 见下面 crlEntryExtensions 组件表 |

crlEntryExtensions 组件：

| CRL 条目扩展 | 是否存在 | 描述 |
|---|---|---|
| reasonCode | 可能 | 撤销原因代码参考下表 CRLReasons。当原因代码为 0 时，不存在；且此原因代码为订户协议中指定的默认提供的选项。当原因代码为其它时，存在且不为关键 |

CRLReasons：

| RFC5280 原因代码 | 值 | 描述 |
|---|---|---|
| 未指定 | 0 | 默认项 |
| 密钥泄漏 | 1 | 确认订户私钥泄漏时使用，如果与下面其它原因有重复时，使用此原因 |
| 隶属关系变更 | 3 | 证书主体名称或者其他主体身份信息变更 |
| 被取代 | 4 | 表示证书正在被替换，因为：订户已请求新证书，CFCA 有合理证据表明证书中任何 FQDN 或 IP 地址的域授权或控制的验证不被证实，或出于合规原因（例如证书不符合这些基准要求或 CPS）而撤销了证书。 |
| 停止运营 | 5 | 表示持有证书的网站在证书到期前被关闭，或者订户在证书到期前不再拥有或控制证书中的域名。 |
| 证书挂起 | 6 | 不适用 |

| | | |
|---|---|---|
| 特权撤销 | 9 | 表示订户方存在未导致密钥泄露的违规行为，例如证书订户在其证书请求中提供了误导性信息，或者未履行订户协议或使用条款下的重大义务。 |

#### 7.2.2.1 CRL 分发点

CFCA 使用完整的 CRL 时候，不使用此扩展。

### 7.3 在线证书状态协议

CFCA 认证系统提供 OCSP 服务，签发的 OCSP 响应符合 RFC6960 标准，该标准定义了一种标准的请求和响应信息格式以确认证书状态。

如果 OCSP 响应中的证书被撤销，在撤销信息中会包含撤销原因。

#### 7.3.1 版本号

RFC6960 定义的 OCSP V1 版本。

#### 7.3.2 OCSP 扩展项

与 RFC6960 一致。

## 8 认证机构审计和其它评估

CFCA 在任何时候都：

1、 遵守 CA/Browser 论坛的 BR 和指南要求。

2、 遵守本章节中规定的 WebTrust 审计要求。

3、 获得工信部授权 CA 运营许可证。

## 8.1 评估的频率或情形

CFCA 在如下情形中进行评估：

1、 年度评估：每年进行一次安全脆弱性评估，对系统、物理场地、运营管理等方面评估，并根据评估报告采取措施，以降低运营风险；

2、 运营质量评估：每年进行一次运营工作质量评估，以保证运营服务的可靠性、安全性和可控性；

3、 运营风险评估：每年进行一次运营风险评估工作，识别内部与外部的威胁，评估威胁事件发生 的可能性及造成的损害，并根据风险评估结果，制定并实施处置计划；

4、 自评估：每年根据 CA/Browser 论坛上 BR 的要求，进行一次 BR 自评估工作；

5、 内部审计：每季度执行一次内部审计，抽取至少 3%的证书样本；

6、 WebTrust 审计：聘请独立的审计师事务所，按照 WebTrust 对 CA 的审计规范，每年进行一次外部审计和评估。

## 8.2 评估者的资质

对 CFCA 的外部审计，由具备以下的资质机构负责：

1、 独立的审计主体；

2、 具备 WebTrust 审计的资质。

3、 必须是经许可的、有执业资格的评估机构,在业界享有良好的声誉。

4、 了解计算机信息安全体系、通信网络安全要求、PKI 技术、标准和操作。

5、 具备检查系统运行性能和信息安全的专业技术和工具。

## 8.3评估者与被评估者的关系

评估者与 CFCA 应无任何业务、财务往来或其它足以影响评估客观性的利害关系。

## 8.4评估内容

1、CFCA 内部评估审核，内容包括：

（1）是否严格按 CP/CPS、业务规范和安全要求开展认证业务。

（2）服务的完整性：密钥和证书生命周期的安全管理、证书撤销的操作、业务系统的安全操作、业务操作规范审查。

（3）物理和环境安全控制：信息安全管理、人员的安全控制、建筑设施的安全控制、软硬件设备和存储介质的安全控制、系统和网络的安全控制、系统开发和维护的安全控制、灾难恢复和备份系统的管理、审计和归档的安全管理等。

2、第三方审计师事务所按照 WebTrust CA 规范的要求，对 CFCA 进行独立审计。

## 8.5对问题与不足采取的措施

对于本机构内部审计结果中的问题，由审计评估小组负责监督相关责任部门的改进情况。

第三方审计师事务所评估完成后，CFCA 按照其工作报告进行整改，并接受再次审计和评估。

## 8.6 评估结果的传达与发布

CFCA 在审计期结束后的三个月内公开审计报告。如果延迟超过三个月，CFCA 提供由合格审计员签署的解释性信函。

审计报告必须包含以下明确标记的信息：

1、 被审计机构的名称。

2、 执行审核机构的名称和地址。

3、 审核范围内的所有根和从属 CA 证书（包括交叉认证的下属 CA 证书）的 SHA-256 指纹。

4、 用于审计每个证书（和相关密钥）的审计标准（包括版本号和关联键）。

5、 审计期间引用的 CA 政策文件列表，以及版本号。

6、 审计评估的是一段时间还是一个时间点。

7、 对于涵盖一段时间的审计，审计期的开始日期和结束日期。

8、 对于针对某个时间点的审计，审计时间点日期。

9、 发布报告的日期，在结束日期或结束日期之后。

CFCA 确保由合格审计员提供公开可用于审计的权威英语版本的审计报告。报告以 PDF 格式提供，并且可通过文本搜索所有所需信息。审计报告中的每个 SHA-256 指纹均是大写字母，并且不包含冒号、空格或换行符。

## 8.7 自我审计

CFCA 将进行持续的自我审核，至少每季度进行一次自我审核，以对自身的服务质量进行控制。自我审核是评估从上次审核期间末至本次审核期间初这段期间内的电子认证活动是否符合相关约定。CFCA 对自身的电子认证活动进

行抽样审查，样本量不得少于此期间内签发证书总数的 3%。

CFCA 采用代码检查（Linting）流程来验证所选样本集中证书的技术准确性，且该流程独立于此前对相同证书所执行的代码检查。

# 9 法律责任和其他业务条款

## 9.1 费用

### 9.1.1 证书签发和更新费用

根据市场和管理部门的规定，CFCA 将收取合理的费用，并在订户向 CFCA 订购证书时，提前告知证书的签发与更新费用。

如果 CFCA 签署的协议中指明的价格和 CFCA 公布的价格不一致，以协议中的价格为准。

### 9.1.2 证书查询费用

CFCA 暂不收取此项收费，但保留对此项服务收费的权利。

### 9.1.3 证书吊销或状态信息的查询费用

CFCA 暂不收取此项收费，但保留对此项服务收费的权利。

### 9.1.4 其它服务费用

CFCA 保留收取其他服务费的权利。

### 9.1.5退款策略

只有 CFCA 违背了本 CP/CPS 所规定的责任与义务，订户可以要求退款。否则，CFCA 对订户收取的费用均不退还。

订户应当提供符合 CFCA 要求的完整、真实、准确的证书申请信息，否则 CFCA 对此造成的损失和后果不承担任何责任。

## 9.2财务责任

### 9.2.1保险范围

CFCA 根据业务发展情况和国内保险公司的业务开展情况决定其投保策略。对于 EV 证书，CFCA 通过了第三方审计公司的财务审计，为计划中的 EV 客户预留了相关的保险金额。

### 9.2.2其它资产

CFCA 确保具有足够的财务实力来维持其正常经营并保证相应义务的履行，并合理地承担对订户及对依赖方的责任。

此要求对证书订户同样适用。

### 9.2.3对最终实体的保险或担保范围

如果 CFCA 根据本 CP/CPS 或任何法律规定，以及司法判定须承担赔偿和/或补偿责任的，CFCA 将按照相关法律法规的规定、仲裁机构的裁定或法院的判决承担相应的赔偿责任。

## 9.3 业务信息保密

### 9.3.1 保密信息范围

保密信息包括但不限于以下内容：

1、CFCA 与订户之间的协议、资料中未公开的内容等属于保密信息。除非法律明文规定或政府、执法机关等的要求，CFCA 承诺不对外公布或透露订户证书信息以外的任何其它隐私信息。

2、订户私钥属于机密信息，订户应当根据本 CP/CPS 的规定妥善保管，如因订户自己泄漏私钥造成的损失，订户应自行承担。

3、审计记录包括:本地日志、服务器日志、归档日志的信息，这些信息被 CFCA 视为保密信息，只有安全审计员和业务管理员可以查看。除法律要求，不可在公司外部发布。

4、其他由 CFCA 保存的个人和公司信息应视为保密，除法律要求，不可公布。

### 9.3.2 不属于保密的信息

不属于保密的信息包括：

1、CA 系统签发的证书信息和 CRL 中的信息。

2、证书、证书内包括的公钥，供用户公开、自由查询和验证。

3、证书被撤销的信息，属于公开信息，CFCA 在目录服务器中公布这些信息。

4、与证书有关的申请流程、申请需要的手续、申请操作指南等信息是可以

公开的。而且 CFCA 在处理申请业务时可以利用这些信息，包括发布上述信息给第三方。

5、其他可以通过公共、公开渠道获得的信息。

### 9.3.3 保护机密信息的责任

CFCA 有各种严格的管理制度、流程和技术手段来保护机密信息，包括但不限于商业机密、客户信息等。CFCA 的每个员工都要接受信息保密方面的培训。

## 9.4 个人信息私密性

### 9.4.1 隐私保密方案

CFCA 尊重所有证书订户个人资料的隐私权，保证完全遵照国家对个人资料隐私保护的相关规定及法律。同时，CFCA 将确保全体职员严格遵从安全和保密标准对个人隐私给予保密。

### 9.4.2 作为隐私处理的信息

CFCA 在管理和使用订户提供的相关信息时，除了证书中已经包括的信息以及证书状态信息外，该订户的基本信息将被视为隐私处理，这些信息将只能由 CFCA 使用，非经订户同意或有关法律法规、公共权力部门根据合法的程序要求，CFCA 不会任意公开。

### 9.4.3不被视作隐私的信息

订户持有的证书信息，以及证书状态信息不被视为隐私信息。

### 9.4.4保护隐私的责任

CFCA、注册机构、订户、依赖方等机构或个人都有义务按照本 CP/CPS 的规定，承担相应的隐私保护责任。在法律法规或公共权力部门通过合法程序要求下，CFCA 可以向特定的对象公布隐私信息，CFCA 无需承担由此造成的任何责任。而且这种披露不能被视为违反了隐私保护义务。如果这种隐私披露导致了任何损失，CFCA 对此不应承担任何责任。

### 9.4.5使用隐私信息的告知与同意

1、CFCA 在其认证业务范围内使用所获得的任何订户信息，只用于订户身份识别、管理、和服务订户的目的。在使用这些信息时，无论是否涉及到隐私，CFCA 都没有告知订户的义务，也无需得到订户的同意。

2、CFCA 在任何法律法规或者法院以及公权力部门通过合法程序的要求下，或者信息所有者书面授权的情况下向特定对象披露隐私信息时，也没有告知订户的义务，并且不需得到订户的同意。

3、认证机构、注册机构如果需要将客户隐私信息用于双方约定的用途以外的目的，事前必须告知订户并获得订户同意和授权，而且这种同意和授权是要用可归档的方式（如传真、信函、电子邮件等）。

### 9.4.6依法律或行政程序的信息披露

除非符合下列条件，CFCA 不会将订户的保密信息提供给其他个人或第三方机构：

1、 司法、行政部门或其他法律法规授权的部门依据政府法律法规、规章\决定、命令等的规定通过合法授权提出的申请。

2、 法院以及公权力部门处理因使用证书产生的纠纷时合法的提出申请。

3、 具有合法司法管辖权的仲裁机构的正式申请。

4、 订户采用授权同意情况下。

5、 本 CP/CPS 规定的其他可以披露的情形。

### 9.4.7其它信息披露情形

CFCA、订户、注册机构、依赖方等机构或个人都有义务按照本 CP/CPS 的规定，承担相应的保护隐私责任。在法律法规或公共权力部门通过合法程序或订户授权同意情况下，CFCA 可以向特定的对象提供隐私信息，CFCA 无需承担由此造成的任何责任。

## 9.5知识产权

1、 CFCA 享有并保留对证书以及 CFCA 提供的全部软件、资料、数据等的著作权、专利申请权等全部知识产权。

2、 CFCA 对数字证书系统软件具有所有权、名称权、利益分享权；

3、 CFCA 有权决定采用何种软件系统。

4、 CFCA 网站上公布的一切信息均为 CFCA 财产，未经 CFCA 书面允许，他人不能转载用于商业行为。

5、 CFCA 发行的证书和 CRL 均为受 CFCA 支配的财产。

6、 对外运营管理策略和规范为 CFCA 财产。

## 9.6陈述与担保

### 9.6.1电子认证服务机构的陈述与担保

CFCA 采用经过国家有关管理机关审批的信息安全基础设施开展电子认证服务业务。

CFCA 的运作遵守《中华人民共和国电子签名法》等法律规定，接受行业主管部门的指导，CFCA 对签发的数字证书承担相应法律责任。

CFCA 的运营遵守 CP/CPS，并随着业务的调整对 CP/CPS 进行修订。

根据《电子认证服务管理办法》要求，CFCA 有责任审计其注册机构电子认证业务是否符合本 CPS 约定。CFCA 对注册机构的审计至少一年一次。CFCA 具有保存和使用证书持有人信息的权限和责任。

### 9.6.2注册机构的陈述与担保

作为 CFCA 的注册机构，应遵照 CFCA 的 CP/CPS 承担电子认证业务中注册机构的职责，其电子认证业务操作受行业及 CFCA 的相关规定管理。

1、注册机构根据 CFCA 制订的策略和运行管理规范，对订户的证书申请材料进行审核，并注册证书订户的信息。通过安全通道将证书订户的信息传送给 CFCA。

2、如注册机构对订户的证书申请材料审查没有通过，注册机构有向订户进行告知的义务。

3、注册机构应在合理的时间内完成证书申请处理。在申请者提交资料齐全且符合要求的情况下，处理证书申请的时间为 1-3 个工作日。

4、注册机构须对订户的信息及与认证相关的信息妥善保存，并于适当的时间转交给 CFCA 归档。注册机构应根据相关协议内容配合 CFCA 需要的电子认证业务合规性审计。

5、注册机构应使订户明确地知道关于使用第三方数字证书的意义、数字证书的功能、使用范围、使用方式、密钥管理以及丢失数字证书的后果和处理措施、法律责任限制，尽到对订户安全提示的义务。

6、注册机构有义务通知订户阅读 CFCA 发布的 CP/CPS 以及其它相关规定，在订户完全知晓并同意 CP/CPS 和《数字证书服务协议》内容的前提下，为订户办理数字证书。

### 9.6.3 订户的陈述与担保

订户确认已经阅读和理解了 CP/CPS 及有关规定的全部内容，并同意受此 CP/CPS 文件规定的约束。

1、订户应遵循诚实、信用原则，在申请数字证书时，应当提供真实、完整和准确的信息和资料，并在这些信息、资料发生改变时及时通知 CFCA。如因订户故意或过失提供的资料不真实、不完整、不准确或资料改变后未及时通知 CFCA，造成的损失由订户自己承担。

2、订户使用 CFCA 数字证书时应使用经合法途径获得的相关软件。

3、订户应通过可靠方式产生密钥对，防止密钥遭受攻击丢失、泄漏和误用；订户应当妥善保管私钥及其保护口令，不得泄漏或交付他人。如因故意或过失导致他人知道、盗用、冒用私钥及其保护口令时，订户应承担由此产生的责任。

4、订户应采取必要手段来保障申请证书时的密钥对中的私钥的安全存储、使用控制、与保密性（包括用于存储私钥的装置或设备），如订户使用的数字证书私钥和密码泄漏、丢失，或者订户不希望继续使用数字证书，或者订户主体不存在时，订户或法定权利人应当立即到原注册机构申请废止该数字证书，相关手续遵循本 CP/CPS 的规定。

5、订户应将证书用于合法目的并符合本 CP/CPS。

6、订户应对使用证书的行为承担责任：

① 使用证书的行为应符合全部适用的法律法规。

② 使用证书的行为应符合订户真实意愿或者仅为了处理已获得授权的事务。

③ 使用证书的行为符合用户协议约定的使用范围和条件。

7、订户在取得证书后应确认证书信息无误。

8、订户保证一旦在证书被吊销后，将不再使用该证书。

9、订户明确了解如果 CFCA 发现了订户证书的不当使用，或者订户证书被用于违法甚至犯罪行为，CFCA 有权直接吊销订户证书。

10、订户损害 CFCA 利益的，须向 CFCA 赔偿全部损失。这些情况包括但不限于：

（1）订户在申请数字证书时没有提供真实、完整、准确的信息，或者在信息变更时未及时通知 CFCA；

（2）订户知道或者应当知道自己的私钥和密码已经失密或者可能已经失密，但未及时告知有关各方且未终止使用；

（3）订户有其他过错或未履行双方约定。

11、订户有按期缴纳数字证书服务费的义务。

12、随着技术的进步，CFCA 有权要求订户更换数字证书。订户在收到数字证书更换通知后，应在规定的期限内向 CFCA 提出更换。因订户逾期没有更换数字证书而引起的后果，由订户自行承担。

### 9.6.4 依赖方的陈述与担保

依赖方声明和承诺：

1、获取并安装该证书对应的证书链。

2、在信赖证书所证明的信任关系前确认该证书为有效证书，包括：检查 CFCA 公布的最新 CRL，确认该证书未被吊销；检查该证书路径中所有出现过的证书的可靠性；检查该证书的有效期；以及检查其他能够影响证书有效性的信息。

3、在信赖证书所证明的信任关系前确认该证书记载的内容与所要证明的内容一致。

4、熟悉本 CP/CPS 的条款，了解证书的使用目的，只在符合本 CP/CPS 规定的证书应用范围内信任该证书。

5、同意 CP/CPS 中关于 CFCA 责任限制的规定。

### 9.6.5其它参与者的陈述与担保

未列明的其他参与者应遵循本 CP/CPS 的规定。

## 9.7担保免责

1、如果证书申请人或订户提供不准确、不真实、不完整的信息，向 CFCA 申请签发证书，那么订户因使用该证书而产生的纠纷，由证书申请人或订户自行承担全部法律责任，CFCA 对此不承担任何责任或后果。

2、由于非 CFCA 原因造成的设备故障、网络中断导致证书报错、交易中断或其他事故造成的损失，CFCA 不向任何方承担赔偿和/或补偿责任。

3、CFCA 对各类证书的适用范围作了规定，若证书被超出范围使用或被用于其他未被 CFCA 允许的用途，CFCA 不承担任何法律责任。

4、由于不可抗力因素导致 CFCA 暂停、终止部分或全部数字证书服务，CFCA 不承担赔偿和/或补偿责任。

5、CFCA 在法律许可的范围内，根据有关法律法规的要求，如实提供电子交易和网络交易中产生的数字签名的验证信息（“验证服务”），对非因该验证服务而导致的任何后果，CFCA 不承担任何法律责任。

6、对于明显由于 CFCA 的合作方的越权行为或其他过错行为所引发的违反约定义务而对订户造成的损失，CFCA 不承担赔偿和/或补偿责任。

## 9.8有限责任

如果 CFCA 根据本 CP/CPS 或任何法律规定，以及司法判定须承担赔偿和/或补偿责任的，CFCA 将按照相关法律法规的规定、仲裁机构的裁定或法院的

判决承担相应的赔偿责任。

## 9.9 CFCA 承担赔偿责任的限制

### 9.9.1 赔偿范围

如 CFCA 违反了本 CP/CPS 9.6.1 中的陈述，证书订户可以申请 CFCA 承担赔偿责任(法定或约定免责除外)。赔偿金额为双方协议规定。

如出现下述情形，CFCA 承担有限赔偿责任:

1、CFCA 将证书错误的签发给订户以外的第三方,导致订户遭受损失的。

2、在 CFCA 明知订户提交信息或资料存在虚假谎报的情况，但仍然向订户签发证书，导致真实实体遭受损失的。

3、由于 CFCA 的原因导致证书私钥被破译、窃取、泄露，导致订户遭受损失的。

4、CFCA 未能及时撤销证书，导致订户遭受损失的。

此外。CFCA 赔偿限制如下：

1、CFCA 所有的赔偿义务不得高于本 CP/CPS 9.2.1,这种赔偿上限可以由 CFCA 根据情况重新制定,CFCA 会将重新制定后的情况立刻通知相关当事人。

2、对于由订户或依赖方的原因造成的损失，CFCA 不承担责任，由订户或依赖方自行承担。

3、CFCA 只有在证书有效期限内承担损失赔偿责任。

### 9.9.2 订户的赔偿责任

如因下述情形而导致 CFCA 或依赖方遭受损失，订户应当承担赔偿责任:

1、订户申请注册证书时，因故意、过失或者恶意提供不真实资料，导致 CFCA 或第三方遭受损害。

2、订户因故意或者过失造成其私钥泄漏、遗失，明知私钥已经泄漏、遗失而没有告知 CFCA，以及不当交付他人使用导致 CFCA 或第三方遭受损害。

3、订户使用证书的行为，有违反本 CP/CPS 及相关操作规范，或者将证书用于非本 CP/CPS 规定的业务范围。

4、证书订户或者其它有权提出撤销证书的实体提出撤销请求后，到 CFCA 将该证书撤销信息予以发布的期间，如果该证书被用以进行非法交易，或者进行交易时产生纠纷的，如果 CFCA 按照本 CP/CPS 的规范进行了有关操作，那么该证书订户必须承担所有损害赔偿责任。

5、提供的资料或信息不真实、不完整或不准确。

6、证书中的信息发生变更但未停止使用证书并及时通知 CFCA 和依赖方。

7、没有对私钥采取有效的保护措施，导致私钥丢失或被损害、窃取、泄露等。

8、在得知私钥丢失或存在危险时，未停止使用证书并及时通知 CFCA 和依赖方。

9、证书到期但仍在使用证书。

10.订户的证书信息侵犯了第三方的知识产权。

11.在规定的范围外使用证书，如从事违法犯罪活动。

### 9.9.3 依赖方的赔偿责任

如因下述情形而导致 CFCA 或订户遭受损失，依赖方应当承担赔偿责任。

1、没有履行 CFCA 与依赖方的协议和本 CP/CPS 中规定的义务。

2、未能依照本 CP/CPS 规范进行合理审核，导致 CFCA 或第三方遭受损害。

3、在不合理的情形下信赖证书，如依赖方明知证书存在超范围、超期限使用的情形或证书已经或有可能被人窃取的情形，但仍然信赖证书。

4、依赖方没有对证书的信任链进行验证。

5、依赖方没有通过查询 CRL 或 OCSP 确认证书是否被撤销。

## 9.10 有效期限与终止

### 9.10.1 有效期限

本 CP/CPS 自 CFCA 在其官方网站（https://www.cfca.com.cn）公布之日起生效，除非 CFCA 特别声明 CP/CPS 提前终止。

### 9.10.2 终止

CFCA 有权终止本 CP/CPS（包括其修订版本），本 CP/CPS（包括其修订版本）自 CFCA 在其官方网站公布终止声明的 30 日后终止。

自新版本的 CP/CPS 在 CFCA 官方网站公布之日起，上一版本的 CP/CPS 效力将自动终止。

### 9.10.3 终止后的存续条款

CP/CPS 中涉及的审计、保密信息、隐私保护、知识产权等方面，以及涉及赔偿的有限责任条款，在本 CP/CPS 终止后继续有效。

## 9.11 对参与者的个别通告与沟通

参与者如需要进一步了解任何本 CP/CPS 中提及的服务、规范、操作等信息，可以通过电话联系 CFCA，联系电话：010-80864610。

## 9.12 修订

CFCA 有权修订本 CP/CPS，并将修订后的版本在官方网站上公布。修订版本自公布之日起生效。

### 9.12.1 修订程序

经 CFCA 安全策略委员会授权，CPS 编写小组每年至少审查一次本 CP/CPS，确保符合国家法律法规和主管部门的要求及相关国际标准，并符合认证业务开的实际需要。

本 CP/CPS 的修改和更新，由 CPS 编写小组提出修订意见，经 CFCA 安全策略委员会批准后，由 CPS 编写小组负责完成修订，修订后的 CP/CPS 经过 CFCA 安全策略委员会批准后正式对外发布。

### 9.12.2 通知机制和期限

CFCA 有权修订本 CP/CPS 中的任何术语和条款，修订后会及时公布在 CFCA 网站上。如在修订发布后 7 个工作日内，订户没有申请对其证书进行吊销，将被视为同意修订后的 CP/CPS。

### 9.12.3 必须修改 OID 的情形

CFCA 在修改认证政策（CP）/ 认证业务声明（CPS）时，会决定是否对对象标识符（OID）进行修改。

## 9.13 争议解决

订户或依赖方在发现或合理怀疑由 CFCA 提供的认证服务造成订户的电子交易信息的泄漏或篡改时，订户可向 CFCA 提出争议处理请求并通知有关各方，或向北京仲裁委申请仲裁。

争议处理流程为：

1、 争议解决的通知：

当争议发生时，在采取任何行动措施之前，订户应首先通知 CFCA。

2、 争议解决的方式：

如果争议在最初通知之日起 10 天内未被解决，CFCA 将召集由 3 名安全认证专家组成外部专家小组。外部专家小组以协助解决争议为目的，收集相关事实。专家小组应在成立之日起 10 天内（除非当事人同意将此段时限延长至一特定时段）完成建议并向当事人传达。专家小组的建议对当事人无约束力，但当事人一方若书面签署文件表示同意该建议，则争议的双方即按照建议的内容解决争议。如果订户在书面签署文件同意专家小组建议后后悔，并将争议提交仲裁，则该建议将视为 CFCA 与订户之间就争议解决达成的协议且受法律保护。

3、 正式争议解决：

若专家小组未能在约定时限内提出有效建议，或者所提的建议不能使双方当事人就争议的解决达成一致意见，争议双方仅可以将争议提交北京仲裁委员

会仲裁。

4、 索赔时限

任何订户或依赖方欲向 CFCA 提出索赔，应自知道或应当知道权力受损之日起的三年内提出。超出三年的，该索赔无效。

## 9.14 管辖法律

CFCA CP/CPS 和协议中条款的制定遵守《中华人民共和国合同法》和《中华人民共和国电子签名法》及相关法律规定。如 CP/CPS 中某项条款与上述法律条款或其可执行性发生抵触，CFCA 将会对此条款进行修改，使之符合相关法律规定。

## 9.15 与适用法律的符合性

CFCA 的各项策略均遵守并符合中华人民共和国各项法律法规和国家信息安全主管部门要求。若本 CP/CPS 的某一条款被主管部门宣布为非法、不可执行或无效时，CFCA 将对该不符合性条款进行修改，直至该条款合法和可执行为止。本 CP/CPS 某一个条款的不可执行性不会影响其它条款的法律效力。

## 9.16 一般条款

### 9.16.1 本 CP/CPS 的完整性

本 CP/CPS 将替代所有以前的或同时期的、与相同主题相关的书面或口头解释。CP/CPS、订户协议及依赖方协议及其补充协议构成各参与者之间的完整协议。

### 9.16.2 转让

CA、RA、订户及依赖方之间的权利义务不能通过任何形式转让给任何人。

### 9.16.3 分割性

本 CP/CPS 的某一条款被主管部门宣布为非法、不可执行或无效时，CFCA 将对该不符合性条款进行修改，直至该条款合法和可执行为止，但此条款的不可执行性不会影响其它条款的有效性。

### 9.16.4 强制执行（律师费与权利放弃）

无。

### 9.16.5 不可抗力

不可抗力是指不能预见、不能避免并不能克服的的客观情况。构成不可抗力的事件包括战争、恐怖行动、罢工、自然灾害、传染性疾病、互联网或其它基础设施无法使用等。但各方都有义务建立灾难恢复和业务连续性机制。

## 9.17 其它条款

CFCA 承诺遵循 CA/Browser Forum(https://www.cabforum.org.)发布的最新版本的《EV 证书指导准则 Guidelines For The Issuance And Management Of Extended Validation Certificates》《公众可信证书签发和管理基线要求 Baseline Requirements for the Issuance andManagement of Publicly-Trusted Certificates》，若 CP/CPS 与以上两个指导准则不符，以准则为准。

## 9.18 最终解释权

本 CPS 最终解释权由 CFCA 所有，由 CFCA 负责解释和修订。

# 10 附录 A CFCA 全球信任体系 CP/CPS 4.8 约束 CA

| NO | 根 CA | 根 CA 算法 | 中级 CA | 中级 CA 算法 |
|---|---|---|---|---|
| 1 | CFCA EV Root | RSA4096/SHA256 | CFCA EV OCA | RSA2048/SHA256 |
| | | | CFCA OV OCA | RSA2048/SHA256 |
| | | | CFCA DV OCA | RSA2048/SHA256 |
| 2 | CFCA Global ECC ROOT G2 | ECC-384（P-384）/SHA384 | CFCA EV ECC OCA G2 | ECC-256/SHA256 |
| | | | CFCA OV ECC OCA G2 | ECC-256/SHA256 |
| | | | CFCA DV ECC OCA G2 | ECC-256/SHA256 |
| 3 | CFCA Global RSA ROOT G2 | RSA4096/SHA256 | CFCA EV RSA OCA G2 | RSA2048/SHA256 |
| | | | CFCA OV RSA OCA G2 | RSA2048/SHA256 |
| | | | CFCA DV RSA OCA G2 | RSA2048/SHA256 |

# 11附录 B 全球信任证书格式

## 11.1 根证书

| 多用途根证书字段 | | 关键扩展项 | 内容 |
|---|---|---|---|
| 版本 | | | V3 |
| 序列号 | | | 包含至少 64 位的 CSPRNG |
| 签发者 | | | 和主题逐字节匹配 |
| TBSCertificate 签名 | | | CFCA Global RSA ROOT G2: sha512withRSA<br>CFCA Global ECC ROOT G2: sha384withECDSA<br>CFCA EV ROOT: sha256withRSA |
| 有效期:notBefore | | | 生成仪式当天 |
| 有效期:notAfter | | | 25 年 |
| 主题 | 通用名称(CN) | | CFCA Global RSA ROOT G2<br>CFCA Global ECC ROOT G2<br>CFCA EV ROOT |
| | 组织(0) | | China Financial Certification Authority |
| | 国家(C) | | CN |
| 公钥信息 | | | CFCA Global RSA ROOT G2 & CFCA EV ROOT<br>: RSA4096<br>(0ID: 1.2.840.113549.1.1.1)<br>CFCA Global ECC ROOT G2<br>: secp384r1 (0ID: 1.3.132.0.34) |
| 签名算法 | | | 与 TBSCertificate 签名匹配 |
| 扩展: authorityKeyIdentifier | | 非关键 | 与 subjectKeyIdentifier 匹配 |
| 扩展:subjectKeyIdentifier | | 非关键 | 根据 RFC 5280，subjectPublicKey 的 160 位 SHA-1 哈希值 |
| 扩股:basicConstraints | | 关键 | Subject Type=CA<br>Path Length Constraint=None |
| 扩展: keyUsage | | 关键 | keyCertSign,cRLSign |

## 11.2 中级证书

| 多用途 PKI 中级证书字段 | 关键扩展项 | 内容 |
|---|---|---|
| 版本 | | V3 |
| 序列号 | | 包含至少 64 位的 CSPRNG |
| 签发者 | | 与签发 CA 的 Subject 信息逐字节匹配 |
| TBSCertificate 签名 | | sha256withRSA |

| | | | |
|---|---|---|---|
| | | | sha512withRSA<br>sha384withECDSA |
| 有效期:notBefore | | | 生成仪式当天 |
| 有效期:notAfter | | | 不晚于签名证书的 notAfter |
| 主题 | 通用名称(CN) | | 见第 1.1.2 章中所述 |
| | 组织(0) | | China Financial Certification Authority |
| | 国家(C) | | CN |
| 公钥算法 | | | RSA4096 (0ID: 1.2.840.113549.1.1.1)<br>or secp384r1 (0ID:1.3.132.0.34) |
| 签名算法 | | | 与 TBSCertificate 签名匹配 |
| 扩展: subjectKeyIdentifier | | 非关键 | 根据 RFC 5280，subjectPublicKey 的 160 位 SHA-1 哈希值 |
| 扩展: authorityKeyIdentifier | | 非关键 | 匹配签名证书的 subjectKeyIdentifier |
| 扩展: certificatePolicies | | 非关键 | 用于签发除上述之外的中级 CA，该扩展为<br>Policy Identifier=Any Policy (2.5.29.32.0) |
| 扩展: basicConstraints | | 关键 l | Subject Type-CA<br>Path Length Constraint=0 |
| 扩展: keyUsage | | 关键 | digitalSignature, keyCertSign, cRlSign |
| 扩展: extKeyUsage | | 非关键 | 必须存在<br>用于签发 SSL/TLS 类型，该扩展为:<br>服务器验证 1.3.6.1.5.5.7.3.1<br>客户端验证 1.3.6.1.5.5.7.3.2<br>用于签发文档签名证书，该扩展为:<br>PDF 签名 1.2.840.113583.1.1.5<br>微软文档签名 1.3.6.1.4.1.311.10.3.12 |
| 扩展: authorityInfoAccess | | 非关键 | ICA AccessMethod=1.3.6.1.5.5.7.48.2<br>OCSP AccessMethod=1.3.6.1.5.5.7.48.1 |
| 扩展: cRLDistributionPoints | | 非关键 | CRL HTTP |

## 11.3 订户证书

| EV SSL全球服务器证书格式 | | | |
|---|---|---|---|
| 证书域 | 域值 | | |
| 版本 | V3 | | |
| 序列号 | 包含至少20位的随机数 | | |
| 签名算法 | SHA256RSA | SHA256RSA | SHA256ECDSA |
| 颁发者 | CN = CFCA EV OCA<br>O = China Financial Certification Authority<br>C = CN | CN = CFCA EV RSA OCA G2<br>O = China Financial Certification Authority<br>C = CN | CN = CFCA EV ECC OCA G2<br>O = China Financial Certification Authority<br>C = CN |
| 有效期起始日期 | 证书有效期起始时间 | | |
| 有效期终止日期 | 证书有效期终止时间 | | |
| 主题 | CN = pu（2）cebnet.com.cn | 必填且只能是域名 | 必填且只能是域名 |

| | | | |
|---|---|---|---|
| | OU = E-banking network | 部门名称，选填<br>（2022年9月1日起不再包含OU） | 部门名称，选填<br>（2022年9月1日起不再包含OU） |
| | O = China E-banking network | 法定的组织机构名称，如使用非官方名称，应能正确反映其组织机构名称，并且不能引起歧义。如名称超过64字节，应使用缩写，但缩写不应引起对机构名称的歧异。 | 法定的组织机构名称，如使用非官方名称，应能正确反映其组织机构名称，并且不能引起歧义。如名称超过64字节，应使用缩写，但缩写不应引起对机构名称的歧异。 |
| | L = Beijing<br>S = Beijing | 营业地址：包括国家、州或省、城市或乡镇、街道号码、邮编。国家、州或省、城市或乡镇是必选项街道号码和邮编是可选项。 | 营业地址：包括国家、州或省、城市或乡镇、街道号码、邮编。国家、州或省、城市或乡镇是必选项<br>街道号码和邮编是可选项。 |
| | C = CN | 国家识别名 | 国家识别名 |
| | SERIALNUMBER = 110000006499259 | 提供的证件注册码（如组织机构代码、企业营业执照代码、税务登记码等），如没有证件注册码，则以成立日期代替。 | 提供的证件注册码（如组织机构代码、企业营业执照代码、税务登记码等），如没有证件注册码，则以成立日期代替。 |
| | 2.5.4.15 = Private Organization | 业务类型：可以是下面的一种<br>Private Organization<br>Government Entity<br>Business Entity<br>Non-Commercial Entity | 业务类型：可以是下面的一种<br>Private Organization<br>Government Entity<br>Business Entity<br>Non-Commercial Entity |
| | 1.3.6.1.4.1.311.60.2.1.1 = 注册地区<br>1.3.6.1.4.1.311.60.2.1.2 = 注册省份<br>1.3.6.1.4.1.311.60.2.1.3 = 注册地所在国家代码 | 注册管辖区地址 | 注册管辖区地址 |
| 公钥 | RSA（2048） | RSA(2048) | ECC 256 |
| 颁发机构访问信息 | [1]Authority Info Access<br>Access Method=联机证书状态协议 (1.3.6.1.5.5.7.48.1)<br>Alternative Name:<br>URL=http://ocsp.cfca.com.cn/ocsp<br>[2]Authority Info Access<br>Access Method=证书颁发机构颁发者 (1.3.6.1.5.5.7.48.2)<br>Alternative Name:<br>URL=http://gt（3）cfca.com.cn/evoca/evoca.cer | | |

| | | | |
|---|---|---|---|
| 颁发机构密钥标识符 | | | |
| 基本限制 | Subject Type=End Entity<br>Path Length Constraint=None | | |
| 证书策略 | [1]Certificate Policy:<br>Policy Identifier=2.16.156.112554.3<br>[1,1]Policy Qualifier Info:<br>Policy Qualifier Id=CPS<br>Qualifier:<br>http://www.cfca.com.cn/us/us-12.htm | | |
| CRL分发点 | [1]CRL Distribution Point<br>Distribution Point Name:<br>Full Name:<br>URL=http://crl.cfca.com.cn/evoca/RSA/crl1.crl | EV证书的CRL分发点 | EV证书的CRL分发点 |
| 密钥用法 | Digital Signature, Key Encipherment (a0) | | |
| 主题密钥标识符 | | | |
| 增强密钥用法 | 服务器验证 (1.3.6.1.5.5.7.3.1) | | |
| 主题备用名 | 域名 | | |

| OV SSL全球服务器证书格式 | | | |
|---|---|---|---|
| 证书域 | 域值 | | |
| 版本 | V3 | | |
| 序列号 | 包含至少20位的随机数 | | |
| 签名算法 | SHA256RSA | SHA256RSA | SHA256ECDSA |
| 颁发者 | CN = CFCA OV OCA<br>O = China Financial Certification Authority<br>C = CN | CN = CFCA OV RSA OCA G2<br>O = China Financial Certification Authority<br>C = CN | CN = CFCA OV ECC OCA G2<br>O = China Financial Certification Authority<br>C = CN |
| 有效期起始日期 | 证书有效期起始时间 | | |
| 有效期终止日期 | 证书有效期终止时间 | | |
| 主题 | CN = pu（2）cebnet.com.cn | 必填且只能是域名或者外网IP | 必填且只能是域名或者外网IP |
| | OU = E-banking network | 部门名称（非必须）<br>（2022年9月1日起不再包含OU） | 部门名称（非必须）<br>（2022年9月1日起不再包含OU） |
| | O = China E-banking network | 法定的组织机构名称，如使用非官方名称，应能正确反映其组织机构名称，并且不能引起歧义。 | 法定的组织机构名称，如使用非官方名称，应能正确反映其组织机构名称，并且不能引起歧义。 |

| | | | |
|---|---|---|---|
| | | 如名称超过64字节，应使用缩写，但缩写不应引起对机构名称的歧异。 | 如名称超过64字节，应使用缩写，但缩写不应引起对机构名称的歧异。 |
| | L = Beijing<br>S = Beijing | 营业地址：包括国家、州或省、城市或乡镇、街道号码、邮编。国家、州或省、城市或乡镇是必选项<br>街道号码和邮编是可选项。 | 营业地址：包括国家、州或省、城市或乡镇、街道号码、邮编。国家、州或省、城市或乡镇是必选项<br>街道号码和邮编是可选项。 |
| | C=CN | 国家代码 | 国家代码 |
| 公钥 | RSA（2048） | RSA（2048） | ECC（256） |
| 颁发机构访问信息 | [1]Authority Info Access<br>Access Method=联机证书状态协议 (1.3.6.1.5.5.7.48.1)<br>Alternative Name:<br>URL=http://ocsp.cfca.com.cn/ocsp<br>[2]Authority Info Access<br>Access Method=证书颁发机构颁发者 (1.3.6.1.5.5.7.48.2)<br>Alternative Name:<br>URL=http://gt（3）cfca.com.cn/ovoca/ovoca.cer | | |
| 颁发机构密钥标识符 | | | |
| 基本限制 | Subject Type=End Entity<br>Path Length Constraint=None | | |
| 证书策略 | [1]Certificate Policy:<br>Policy Identifier=2.16.156.112554.3.2<br>[1,1]Policy Qualifier Info:<br>Policy Qualifier Id=CPS<br>Qualifier:<br>http://www.cfca.com.cn/us/us-12.htm | | |
| CRL分发点 | [1]CRL Distribution Point<br>Distribution Point Name:<br>Full Name:<br>URL=<br>http://crl.cfca.com.cn/OVOCA/RSA/crl1.crl | 证书的CRL分发点 | 证书的CRL分发点 |
| 密钥用法 | Digital Signature, Key | | |

| | | | |
|---|---|---|---|
| | Encipherment (a0) | | |
| 主题密钥标识符 | | | |
| 增强密钥用法 | 客户端验证 (1.3.6.1.5.5.7.3.2)<br>服务器验证 (1.3.6.1.5.5.7.3.1) | | |
| 主题备用名 | 外网ip或者域名 | | |

| DV SSL全球服务器证书格式 | | | |
|---|---|---|---|
| 证书域 | 域值 | | |
| 版本 | V3 | | |
| 序列号 | 包含至少20位的随机数 | | |
| 签名算法 | SHA256RSA | SHA256RSA | SHA256ECDSA |
| 颁发者 | CN = CFCA DV OCA<br>O = China Financial Certification Authority<br>C = CN | CN = CFCA DV RSA OCA G2<br>O = China Financial Certification Authority<br>C = CN | CN = CFCA DV ECC OCA G2<br>O = China Financial Certification Authority<br>C = CN |
| 有效期起始日期 | 证书有效期起始时间 | | |
| 有效期终止日期 | 证书有效期终止时间 | | |
| 主题 | CN = pu（2）cebnet.com.cn | 必填且只能是域名或者外网IP | 必填且只能是域名或者外网IP |
| | C=CN | 国家代码 | 国家代码 |
| 公钥 | RSA（2048） | RSA（2048） | ECC（256） |
| 颁发机构访问信息 | [1]Authority Info Access<br>Access Method=联机证书状态协议 (1.3.6.1.5.5.7.48.1)<br>Alternative Name:<br>URL=http://ocsp.cfca.com.cn/ocsp<br>[2]Authority Info Access<br>Access Method=证书颁发机构颁发者 (1.3.6.1.5.5.7.48.2)<br>Alternative Name:<br>URL=http://gt（3）cfca.com.cn/ovoca/ovoca.cer | | |
| 颁发机构密钥标识符 | | | |
| 基本限制 | Subject Type=End Entity<br>Path Length Constraint=None | | |
| 证书策略 | [1]Certificate Policy:<br>Policy Identifier=2.16.156.112554.3.2<br>[1,1]Policy Qualifier Info:<br>Policy Qualifier | | |

| | | | |
|---|---|---|---|
| | Id=CPS<br>Qualifier:<br>http://www.cfca.com.cn/us/us-12.htm | | |
| CRL分发点 | [1]CRL Distribution Point<br>Distribution Point Name:<br>Full Name:<br>URL=<br>http://crl.cfca.com.cn/evoca/RSA/crl1.crl | [1]CRL Distribution Point<br>Distribution Point Name:<br>Full Name:<br>URL=<br>http://crl.cfca.com.cn/eccroot/RSA/crl1.crl | [1]CRL Distribution Point<br>Distribution Point Name:<br>Full Name:<br>URL=<br>http://crl.cfca.com.cn/eccroot/ECC/crl1.crl |
| 密钥用法 | Digital Signature, Key Encipherment (a0) | | |
| 主题密钥标识符 | | | |
| 增强密钥用法 | 客户端验证 (1.3.6.1.5.5.7.3.2)<br>服务器验证 (1.3.6.1.5.5.7.3.1) | | |
| 主题备用名 | 外网ip或者域名 | | |

## 11.4 OCSP 签名证书

| 证书字段 | | Critical Extension | Contents |
|---|---|---|---|
| 版本 | | | V3 |
| 序列号 | | | 包含至少 64 位的 CSPRNG |
| TBSCertificate 签名 | | | |
| 签发者 | | | 与签发 CA 的 Subject 逐字节匹配 |
| 有效期:notBefore | | | 距签发时间相差不超过 24 小时 |
| 有效期:notAfter | | | 不超过 398 天 |
| 主题 | 通用名称(CN) | | |
| | 组织(0) | | China Financial Certification Authority |
| | 国家(C) | | CN |
| 公钥信息 | | | RSA2048 \| 3072 \| 4096 or ECDSA P-256 \| P-384 |
| 签名算法 | | | 和 TBSCertificate 匹配 |
| 扩展：subjectKeyIdentifier | | 非关键 | 根据 RFC 5280,subjectPublicKey 的 160 位 SHA-1 哈希值 |
| 扩展：authorityKeyIdentifier | | 非关键 | 匹配签名证书的 subjectKeyIdentifier |
| 扩展：basicConstraints | | 关键 | Subject Type=End Entity<br>Path Length Constraint=None |
| 扩展：keyUsage | | 关键 | digitalSignature |
| 扩展：extKeyUsage | | 非关键 | OCSP 签名(1.3.6.1.5.5.7.3.9) |
| 扩展：<br>id-pkix-ocsp-nocheck(1.3.6.1.5.5.7.48.1.5) | | 非关键 | 0x0500 |